在线学习资料支持

您可以在华为企业业务网站获得E-Learning课程、培训教材 、产品资料、软件工具、技术案例等：

1、 **E-Learning课程：**登录*华为在线学习网站*，进入“*华为培训/在线学习*”栏目

免费E-Learning课：对网站所有用户免费开放

职业认证E-Learning课：通过任何一项职业认证即可学习所有职业认证培训E-Learning课程

渠道赋能E-Learning课：对华为企业业务合作伙伴免费开放

2、**培训教材：**登录*华为在线学习网站*，进入“*华为培训/面授培训*”，在具体课程页面即可下载教材。

华为职业认证培训教材、华为产品技术培训教材。无需注册即可下载

3、**华为在线公开课(LVC)：** http://support.huawei.com/ecommunity/bbs/10154479.html

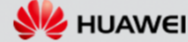
企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师公开授课

4、**产品资料下载：** http://support.huawei.com/enterprise/#tabname=productsupport

5、**软件工具下载：** http://support.huawei.com/enterprise/#tabname=softwaredownload

更多内容请访问：

- http://learning.huawei.com/cn
- http://support.huawei.com/enterprise/
- http://support.huawei.com/ecommunity/



华为认证系列教程

HCDP-IENP
提升企业级网络性能
实验指导书



华为技术有限公司

版权声明

华为认证系列教程

HCDP-IENP提升企业级网络性能

实验指导书

第1.6版本

华为认证体系介绍

依托华为公司雄厚的技术实力和专业的培训体系，华为认证考虑到不同客户对ICT技术不同层次的需求，致力于为客户提供实战性、专业化的技术认证。

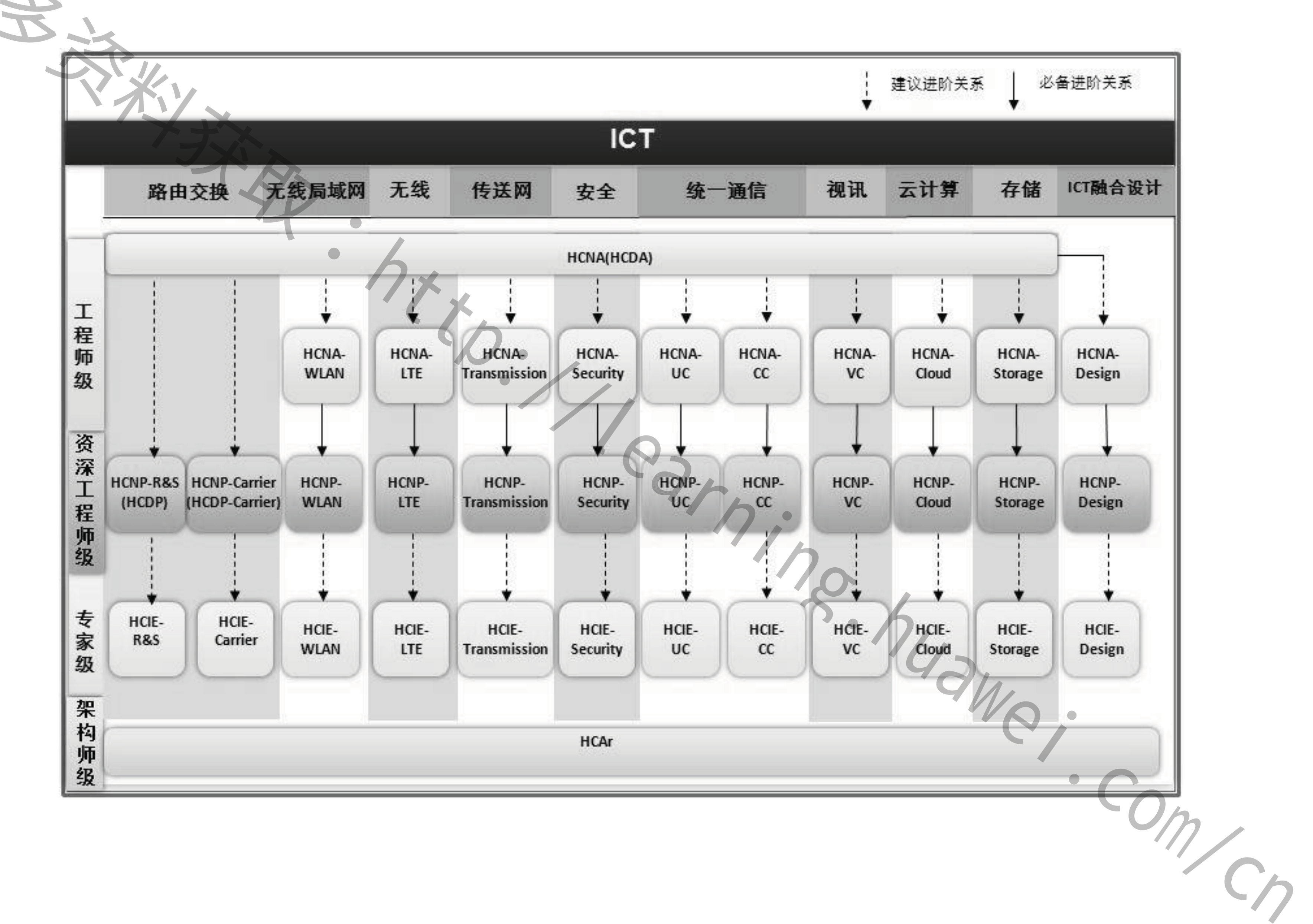
根据ICT技术的特点和客户不同层次的需求，华为认证为客户提供面向十三个方向的四级认证体系。

HCNA(HCDA)认证定位于中小型网络的基本配置和维护。HCNA(HCDA)认证包括但不限于：网络基础知识；流行网络的基本连接方法；基本的网络建造；基本的网络故障排除；华为路由交换设备的安装和调试。通过HCNA(HCDA)认证，将证明您对中小型网络有初步的了解，了解面向中小型企业的网络通用技术，并具备协助设计中小企业网络以及使用华为路由交换设备实施设计的能力。拥有通过HCNA(HCDA)认证的工程师，意味着中小企业有能力完成基本网络搭建，并将基本的语音、无线、云、安全和存储集成到网络之中，满足各种应用对网络的使用需求。

HCNP-Enterprise (HCDP-Enterprise)认证定位于中小型网络的构建和管理。HCNP-Enterprise (HCDP-Enterprise)认证包括但不限于：网络基础知识；交换机和路由器原理；TCP/IP 协议簇；路由协议；访问控制；网络故障的排除；华为路由交换设备的安装和调试。通过HCNP-Enterprise (HCDP-Enterprise)认证，将证明您对中小型网络有全面深入的了解，掌握面向中小型企业的网络通用技术，并具备独立设计中小企业网络以及使用华为路由交换设备实施设计的能力。拥有通过HCNP-Enterprise (HCDP-Enterprise)认证的工程师，意味着中小企业有能力完成完整网络的搭建，将企业中所需的语音、无线、云、安全和存储全面地集成到网络之中，并且能满足各种应用对网络的使用需求，进而提供较高的安全性、可用性和可靠性。

HCIE-Enterprise 认证定位于大中型复杂网络的构建、优化和管理。HCIE-Enterprise 认证包括但不限于：不同网络和各种路由器交换机之间的互联；复杂连接问题的解决；使用技术解决方案提高带宽、缩短相应时间、最大限度地提高性能、加强安全性和支持全球应用；复杂网络的故障排除。通过HCIE-Enterprise 认证，将证明您对大型网络有全面深入的了解，掌握面向大型企业网络的技术，并具备独立设计各种企业网络以及使用华为路由交换设备实施设计的能力。拥有通过HCIE-Enterprise 认证的工程师，意味着大中企业有能力独立完成完整的网络搭建，将企业中所需的语音、无线、云、安全和存储全面地集成到网络之中，并且能满足各种应用对网络的使用需求；能够提供完整的故障排除能力；能根据企业和网络技术的发展，规划企业网络的发展，并提供高安全性、可用性和可靠性。

华为认证协助您打开行业之窗，开启改变之门，屹立在ICT世界的潮头浪尖！


建议进阶关系
必备进阶关系
ICT
路由交换
无线局域网
无线
传送网
安全
统一通信
视讯
云计算
存储
ICT融合设计
工程师级
资深工程师级
专家级
架构师级
HCNA(HCDA)
HCNA-WLAN
HCNA-LTE
HCNA-Transmission
HCNA-Security
HCNA-UC
HCNA-CC
HCNA-VC
HCNA-Cloud
HCNA-Storage
HCNA-Design
HCNP-R&S (HCDP)
HCNP-Carrier (HCDP-Carrier)
HCNP-WLAN
HCNP-LTE
HCNP-Transmission
HCNP-Security
HCNP-UC
HCNP-CC
HCNP-VC
HCNP-Cloud
HCNP-Storage
HCNP-Design
HCIE-R&S
HCIE-Carrier
HCIE-WLAN
HCIE-LTE
HCIE-Transmission
HCIE-Security
HCIE-UC
HCIE-CC
HCIE-VC
HCIE-Cloud
HCIE-Storage
HCIE-Design
HCAr

本书常用图标



路由器



三层交换机



二层交换机



防火墙

网云

以太网线缆

串行线缆

实验环境说明

组网介绍

本实验环境面向准备HCDP-IENP考试的网络工程师，实验设备包括路由器5台，交换机4台，防火墙2台。每套实验环境适用于2名学员同时上机操作。

设备介绍

为了满足HCDP-IENP实验需要，建议每套实验环境采用以下配置：

设备名称、型号与版本的对应关系如下：

设备名称	设备型号	软件版本
R1	AR 2220	Version 5.90 (V200R001C01SPC300)
R2	AR 2220	Version 5.90 (V200R001C01SPC300)
R3	AR 2220	Version 5.90 (V200R001C01SPC300)
R4	AR 1220	Version 5.90 (V200R001C01SPC300)
R5	AR 1220	Version 5.90 (V200R001C01SPC300)
S1	S5700-28C-EI-24S	Version 5.70 (V100R006C00SPC800)
S2	S5700-28C-EI-24S	Version 5.70 (V100R006C00SPC800)
S3	S3700-28TP-EI-AC	Version 5.70 (V100R006C00SPC800)
S4	S3700-28TP-EI-AC	Version 5.70 (V100R006C00SPC800)
FW1	USG2160	Version 5.30 (V300R001C00SPC700)
FW2	USG2160	Version 5.30 (V300R001C00SPC700)

目录



第一章 防火墙特性功能

实验 1-1 USG 防火墙安全区域及其他基本功能配置

学习目的

- 掌握防火墙安全区域的配置方法
- 掌握域间包过滤的配置方法
- 掌握在静态与动态配置黑名单的方法
- 掌握黑名单的配置方法
- 掌握应用层包过滤的配置方法

拓扑图

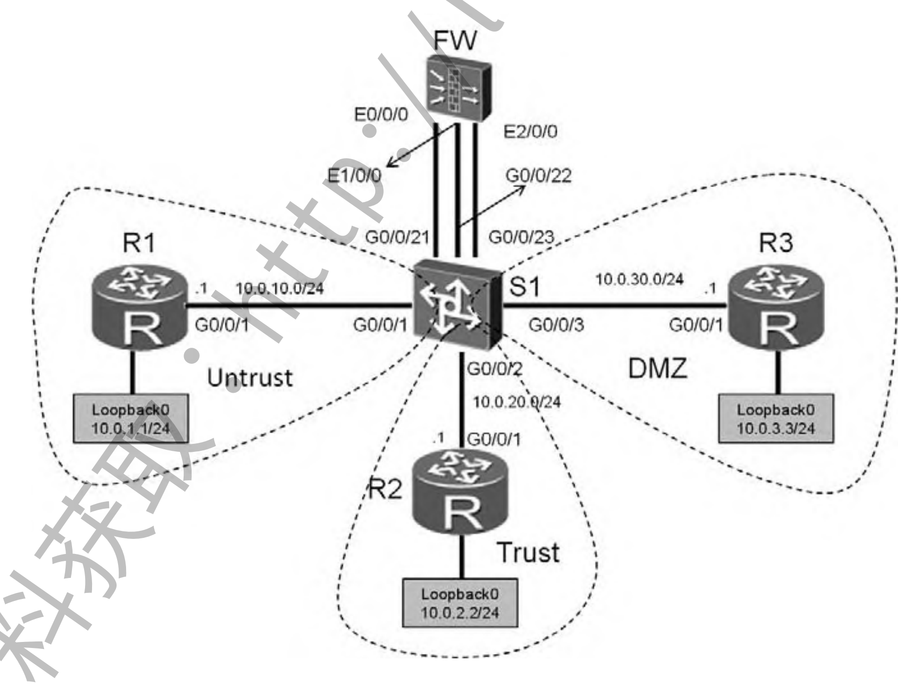


图1-1 USG防火墙区域配置

场景

你是你们公司的网络管理员。公司总部的网络分成了三个区域，包括内部区域（Trust）、外部区域（Untrust）和服务器区域（DMZ）。你设计通过防火墙来实现对数据的控制，添加黑名单来防范网络攻击，确保公司内部网络安全。

学习任务

步骤一. 基本配置与 IP 编址

给三个路由器配置地址信息。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.10.1 24
[R1-GigabitEthernet0/0/1]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.20.1 24
[R2-GigabitEthernet0/0/1]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.30.1 24
[R3-GigabitEthernet0/0/1]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

给防火墙配置地址时，需要注意Ethernet1/0/0接口为二层交换机接口，无法配置IP地址。实验中我们在防火墙上配置VLAN12，定义Vlanif12，配置IP地址作为Inside区域的网关。

由于默认情况下，防火墙会给它的Vlanif1配置地址，实验中为避免干扰，删除该配置。



```
<USG2100>system-view
Enter system view, return user view with Ctrl+Z.
[USG2100]sysname FW
[FW]vlan 12
[FW-vlan-12]quit
[FW]interface vlanif 12
[FW-Vlanif12]ip address 10.0.20.254 24
[FW-Vlanif12]quit
[FW]interface Ethernet 1/0/0
[FW-Ethernet1/0/0]port  access vlan 12
[FW-Ethernet1/0/0]interface Ethernet 0/0/0
[FW-Ethernet0/0/0]ip address 10.0.10.254 24
[FW-Ethernet0/0/0]interface ethernet 2/0/0
[FW-Ethernet2/0/0]ip address 10.0.30.254 24
[FW-Ethernet2/0/0]quit
[FW]interface Vlanif 1
[FW-Vlanif1]undo ip address
```

交换机上需要按照需求定义VLAN。

```
[Quidway]sysname S1
[S1]vlan batch 11 to 13
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 11
[S1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 12
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 13
[S1-GigabitEthernet0/0/3]interface GigabitEthernet 0/0/21
[S1-GigabitEthernet0/0/21]port link-type access
[S1-GigabitEthernet0/0/21]port default vlan 11
[S1-GigabitEthernet0/0/21]interface GigabitEthernet 0/0/22
[S1-GigabitEthernet0/0/22]port link-type access
[S1-GigabitEthernet0/0/22]port default vlan 12
[S1-GigabitEthernet0/0/22]interface GigabitEthernet 0/0/23
[S1-GigabitEthernet0/0/23]port link-type access
[S1-GigabitEthernet0/0/23]port default vlan 13
```

防火墙上默认有四个区域，分别是“local ”、” trust ”、” untrust ”、” dmz ”。实验中我们使用到“trust ”、” untrust “和”dmz “三个区域，分别将对应接口加入各安全区域。

```
[FW]firewall zone dmz
[FW-zone-dmz]add interface Ethernet 2/0/0
[FW-zone-dmz]firewall zone trust
[FW-zone-trust]add interface Vlanif 12
[FW-zone-trust]firewall zone untrust
[FW-zone-untrust]add interface Ethernet 0/0/0
```

查看默认情况下，区域之间是否可以正常通讯。

```
[FW]display firewall packet-filter default all
10:28:18  2011/12/24
 Firewall default packet-filter action is :
 packet-filter in public:
   local -> trust :
     inbound  : default: permit; || IPv6-acl: null
     outbound : default: permit; || IPv6-acl: null
   local -> untrust :
     inbound  : default: deny; || IPv6-acl: null
     outbound : default: permit; || IPv6-acl: null
   local -> dmz :
     inbound  : default: deny; || IPv6-acl: null
     outbound : default: permit; || IPv6-acl: null
   trust -> untrust :
     inbound  : default: deny; || IPv6-acl: null
     outbound : default: deny; || IPv6-acl: null
   trust -> dmz :
     inbound  : default: deny; || IPv6-acl: null
     outbound : default: deny; || IPv6-acl: null
   dmz -> untrust :
     inbound  : default: deny; || IPv6-acl: null
     outbound : default: deny; || IPv6-acl: null

 packet-filter between VFW:
```

由以上显示的内容看出，缺省情况下，Local安全区域和Trust安全区域间的所有方向都允许报文通过，Local安全区域和Untrust安全区域出方向，Local安全区域和DMZ安全区域出方向允许报文通过，其他区域间所有方向都不允许报文通过。

验证区域之间的连通性。

Untrust区域到Trust区域。

```
<R1>ping -a 10.0.1.1 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
```

```
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Untrust区域到DMZ区域。

```
<R1>ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Trust区域到Untrust区域。

```
<R2>ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Trust区域到DMZ区域。

```
<R2>ping -a 10.0.2.2 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
```

```
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

DMZ区域到Untrust区域。

```
<R3>ping -a 10.0.3.3 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break

    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

DMZ区域到Trust区域。

```
<R3>ping -a 10.0.3.3 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

在FW设备上测试到R1，R2，R3的连通性。

```
[FW]ping 10.0.10.1
```

```
 PING 10.0.10.1: 56  data bytes, press CTRL_C to break
   Request time out
   Reply from 10.0.10.1: bytes=56 Sequence=2 ttl=255 time=1 ms
   Reply from 10.0.10.1: bytes=56 Sequence=3 ttl=255 time=1 ms
   Reply from 10.0.10.1: bytes=56 Sequence=4 ttl=255 time=1 ms
   Reply from 10.0.10.1: bytes=56 Sequence=5 ttl=255 time=1 ms

 --- 10.0.10.1 ping statistics ---
   5 packet(s) transmitted
   4 packet(s) received
   20.00% packet loss
   round-trip min/avg/max = 1/1/1 ms

[FW]ping 10.0.20.1
 PING 10.0.20.1: 56  data bytes, press CTRL_C to break
   Request time out
   Reply from 10.0.20.1: bytes=56 Sequence=2 ttl=255 time=1 ms
   Reply from 10.0.20.1: bytes=56 Sequence=3 ttl=255 time=1 ms
   Reply from 10.0.20.1: bytes=56 Sequence=4 ttl=255 time=1 ms
   Reply from 10.0.20.1: bytes=56 Sequence=5 ttl=255 time=1 ms

 --- 10.0.20.1 ping statistics ---
   5 packet(s) transmitted
   4 packet(s) received
   20.00% packet loss
   round-trip min/avg/max = 1/1/1 ms

[FW]ping 10.0.30.1
 PING 10.0.30.1: 56  data bytes, press CTRL_C to break
   Request time out
   Reply from 10.0.30.1: bytes=56 Sequence=2 ttl=255 time=1 ms
   Reply from 10.0.30.1: bytes=56 Sequence=3 ttl=255 time=1 ms
   Reply from 10.0.30.1: bytes=56 Sequence=4 ttl=255 time=1 ms
   Reply from 10.0.30.1: bytes=56 Sequence=5 ttl=255 time=1 ms

 --- 10.0.30.1 ping statistics ---
   5 packet(s) transmitted
   4 packet(s) received
   20.00% packet loss
   round-trip min/avg/max = 1/1/1 ms
```

在R1、R2和R3上配置缺省路由，在FW上配置明确的静态路由，配置区域之间的缺省包过滤策略为允许所有，实现三个Loopback0接口连接的网段之间的

互通。

```
[R1]ip route-static 0.0.0.0 0 10.0.10.254

[R2]ip route-static 0.0.0.0 0 10.0.20.254

[R3]ip route-static 0.0.0.0 0 10.0.30.254

[FW]ip route-static 10.0.1.0 24 10.0.10.1
[FW]ip route-static 10.0.2.0 24 10.0.20.1
[FW]ip route-static 10.0.3.0 24 10.0.30.1
[FW]firewall packet-filter default permit all
```

配置完成后，测试各路由器Loopback0接口连接的网段之间的通讯情况。

```
[R1]ping -a 10.0.1.1 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.2.2: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 10.0.2.2: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.2.2: bytes=56 Sequence=3 ttl=254 time=4 ms
    Reply from 10.0.2.2: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 10.0.2.2: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/3/4 ms

[R1]ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=4 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=254 time=4 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=254 time=4 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=254 time=4 ms

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/4 ms
```

步骤二. 配置域间包过滤

包过滤是一个基础安全策略，主要控制域间报文转发，在进行其他安全策略检查之前都会先进行包过滤规则的检查，所以包过滤功能是否配置正确，将影响设备大部分功能的使用。

配置区域之间的缺省包过滤策略，仅允许Trust区域访问其他区域，不允许其他区域之间的访问。

```
[FW]firewall packet-filter default deny all
[FW]firewall packet-filter default permit interzone trust untrust direction
outbound
[FW]firewall packet-filter default permit interzone trust dmz direction outbound
[FW]firewall session link-state check
```

配置完成后，测试区域之间的连通性。

Untrust区域到Trust区域。

```
[R1]ping -a 10.0.1.1 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Untrust区域到DMZ区域。

```
[R1]ping -a 10.0.1.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
```

```
    100.00% packet loss
```

Trust区域到Untrust区域。

```
[R2]ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms
```

Trust区域到DMZ区域。

```
[R2]ping -a 10.0.2.2 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=5 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=254 time=4 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/5 ms
```

DMZ区域到Untrust区域。

```
[R3]ping -a 10.0.3.3 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.1.1 ping statistics ---
```

```
   5 packet(s) transmitted
   0 packet(s) received
   100.00% packet loss
```

DMZ区域到Trust区域。

```
[R3]ping -a 10.0.3.3 10.0.2.2
  PING 10.0.2.2: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.2.2 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

配置域间包过滤策略，允许Untrust区域访问DMZ区域的特定服务器。

DMZ区域有一台服务器，IP地址为10.0.3.3，需要对Untrust区域开放Telnet服务。同时为了测试网络，需要开放ICMP Ping测试功能。

```
[FW]policy interzone dmz untrust inbound
[FW-policy-interzone-dmz-untrust-inbound]policy 1
[FW-policy-interzone-dmz-untrust-inbound-1]policy service service-set icmp
[FW-policy-interzone-dmz-untrust-inbound-1]policy destination 10.0.3.3 0
[FW-policy-interzone-dmz-untrust-inbound-1]action permit
[FW-policy-interzone-dmz-untrust-inbound-1]quit
[FW-policy-interzone-dmz-untrust-inbound]policy 2
[FW-policy-interzone-dmz-untrust-inbound-2]policy service service-set telnet
[FW-policy-interzone-dmz-untrust-inbound-2]policy destination 10.0.3.3 0
[FW-policy-interzone-dmz-untrust-inbound-2]action permit
[FW-policy-interzone-dmz-untrust-inbound-2]quit
[FW-policy-interzone-dmz-untrust-inbound]policy 3
[FW-policy-interzone-dmz-untrust-inbound-3]action deny
```

为了进行Telnet测试，在R3上开启Telnet功能。

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode none
```

测试网络连通性。

```
<R1>ping 10.0.3.3
```

```
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=254 time=2 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=254 time=2 ms
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=254 time=4 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=254 time=2 ms

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/4 ms

<R1>ping 10.0.30.1
  PING 10.0.30.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.30.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

<R1>telnet 10.0.3.3
  Press CTRL_] to quit telnet mode
  Trying 10.0.3.3 ...
  Connected to 10.0.3.3 ...
<R3>quit

  Configuration console exit, please retry to log on

  The connection was closed by the remote host
<R1>telnet 10.0.30.3
  Press CTRL_] to quit telnet mode
  Trying 10.0.30.3 ...
```

步骤三. 配置黑名单

黑名单仅对IP地址进行识别，能够以很高的速度实现黑名单表项匹配，从而快速有效地屏蔽特定IP地址的用户。黑名单是一个重要的安全特性，其特点为可以由设备动态地进行添加或删除。同包过滤功能相比，黑名单功能的匹配和屏蔽的速度更快，消耗的系统资源更少。如果认为某个IP地址对应的用户不可信时，可将该用户的IP地址加入黑名单，之后当设备收到源地址为该IP地址的报文时，将其予以丢弃，从而达到保护网络安全的目的。

最近发现Untrust区域上不断有不同的IP地址在对公司进行端口扫描，需要对其进行防范。

其中有一个IP地址10.0.111.1已经进行了多次攻击，希望直接屏蔽掉从该IP发来的流量。

在R1上添加环回口，模拟攻击源。并在防火墙上配置静态路由。

```
[R1]interface LoopBack 1
[R1-LoopBack1]ip address 10.0.111.1 24

[FW]ip route-static 10.0.111.0 24 10.0.10.1
```

配置端口扫描攻击防范，使端口扫描攻击的检测结果可以被自动导入到黑名单中。

```
[FW]firewall defend port-scan enable
```

配置IP地址扫描速率的阈值为5000pps。这里的阈值指某个源地址到同一目的地址的IP报文中端口的变化速率。如果这个速率过快，说明这个源地址极可能在扫描目的地址的所有端口。

```
[FW]firewall defend port-scan max-rate 5000
```

配置黑名单超时时间为30分钟。这样攻击防范功能所生成的动态黑名单表项将在30分钟后被删除。

```
[FW]firewall defend port-scan blacklist-timeout 30
```

添加静态黑名单之前，IP地址为10.0.111.1的环回口能够与R3的环回口通讯。

检测连通性。

```
[R1]ping -a 10.0.111.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.3.3: bytes=56 Sequence=1 ttl=254 time=4 ms
    Reply from 10.0.3.3: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=3 ttl=254 time=3 ms
```

```
    Reply from 10.0.3.3: bytes=56 Sequence=4 ttl=254 time=3 ms
    Reply from 10.0.3.3: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/4 ms
```

配置静态黑名单功能，将IP地址10.0.111.1加入黑名单，始终丢弃其发来的报文，直至手工将其从黑名单中删除。

```
[FW]firewall blacklist enable
[FW]firewall blacklist item 10.0.111.1
```

测试连通性。

```
[R1]ping -a 10.0.111.1 10.0.3.3
  PING 10.0.3.3: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.3.3 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

步骤四. 配置应用层包过滤（ASPF）

在多通道协议和NAT的应用中，ASPF是重要的辅助功能。

通过配置ASPF功能，可实现内网正常对外提供FTP和TFTP服务，同时还可避免内网用户在访问外网Web服务器时下载危险控件。

公司提供FTP、TFTP服务，公司员工还需要访问外网的Web网站。在向内网开放的Web网站上可能存在危险的java控件。由于FTP协议为系统预定义协议，只需在域间应用detect ftp即可实现FTP报文的正常转发。而TFTP协议在系统中没有预先定义，可以通过自定义的三元组ASPF来进行匹配。

创建ACL。

ACL3001用于定义访问内网TFTP服务器的流量。由于TFTP服务需要自定义端口号等信息，所以需要单独创建一条ACL。

```
[FW]acl 3001
[FW-acl-adv-3001]rule permit udp destination-port eq tftp
[FW-acl-adv-3001]quit
```

在域间应用对FTP的检查，实现FTP报文的正常转发。应用**detect user-define**，实现TFTP报文的正常转发。

```
[FW]firewall interzone trust dmz
[FW-interzone-trust-dmz]detect ftp
[FW-interzone-trust-dmz]detect user-defined 3001 outbound
[FW-interzone-trust-dmz]quit
```

在域间应用**detect java-blocking**，阻止危险java控件的下载。

```
[FW]firewall interzone trust untrust
[FW-interzone-trust-untrust]detect java-blocking
[FW-interzone-trust-untrust]quit
```

由于ASPF功能决定了很多特殊协议能够得到正常转发，所以当这些业务出现问题时，可以通过如下方式来进行问题定位。

执行命令**display interzone**查看域间的配置，核对域间是否正确配置了ASPF功能。

```
[FW]display interzone
15:42:11  2011/12/25
interzone trust untrust
 detect java-blocking
#
interzone trust dmz
 detect ftp
 detect user-defined 3001 outbound
#
```

附加实验：思考并验证

思考一下，在企业网络中，如果用户和服务都非常多，网络设计时该如何设计？同时可以采用什么方法简化配置？

最终设备配置

```
[R1]display current-configuration
[V200R001C00SPC200]
#
 sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.10.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.0.111.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.10.254
#
return

[R2]display current-configuration
[V200R001C00SPC200]
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
#
return

[R3]display current-configuration
[V200R001C00SPC200]
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.30.1 255.255.255.0
#
```

```
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.30.254
#
return

[FW]display current-configuration
#
 sysname FW
#
 firewall packet-filter default permit interzone trust untrust direction outbound
 firewall packet-filter default permit interzone trust dmz direction outbound
#
 vlan batch 1 12
#
 firewall defend port-scan enable
 firewall defend port-scan max-rate 5000
 firewall defend port-scan blacklist-timeout 30
#
 firewall statistic system enable
#
acl number 3001
 rule 5 permit udp destination-port eq tftp
#
interface Vlanif12
 ip address 10.0.20.254 255.255.255.0
#
interface Ethernet0/0/0
 ip address 10.0.10.254 255.255.255.0
#
interface Ethernet1/0/0
 portswitch
 port link-type access
 port access vlan 12
#
interface Ethernet2/0/0
 ip address 10.0.30.254 255.255.255.0
#
firewall zone local
 set priority 100
#
firewall zone trust
```

```
 set priority 85
 add interface Ethernet1/0/0
 add interface Ethernet1/0/1
 add interface Ethernet1/0/2
 add interface Ethernet1/0/3
 add interface Ethernet1/0/4
 add interface Ethernet1/0/5
 add interface Ethernet1/0/6
 add interface Ethernet1/0/7
 add interface Vlanif1
 add interface Vlanif12
#
firewall zone untrust
 set priority 5
 add interface Ethernet0/0/0
#
firewall zone dmz
 set priority 50
 add interface Ethernet2/0/0
#
firewall interzone trust untrust
 detect java-blocking
#
firewall interzone trust dmz
 detect ftp
 detect user-defined 3001 outbound
#
 ip route-static 10.0.1.0 255.255.255.0 10.0.10.1
 ip route-static 10.0.2.0 255.255.255.0 10.0.20.1
 ip route-static 10.0.3.0 255.255.255.0 10.0.30.1
 ip route-static 10.0.111.0 255.255.255.0 10.0.10.1
#
 firewall blacklist enable
 firewall blacklist item 10.0.111.1
#
policy interzone dmz untrust inbound
 policy 1
  action permit
  policy service service-set icmp
  policy destination 10.0.3.3 0

 policy 2
  action permit
```

```
  policy service service-set telnet
  policy destination 10.0.3.3 0

 policy 3
  action deny
#
return

[S1]display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S1
#
 vlan batch 11 to 13
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 13
#
interface GigabitEthernet0/0/21
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 13
#
return
```

实验 1-2 USG 防火墙 IPSec VPN 配置

学习目的

- 掌握在USG防火墙上配置IPSec VPN的方法
- 掌握在USG防火墙上配置GRE over IPSec VPN的方法
- 掌握在路由器上配置IPSec VPN的方法
- 掌握在路由器上配置GRE over IPSec VPN的方法

拓扑图

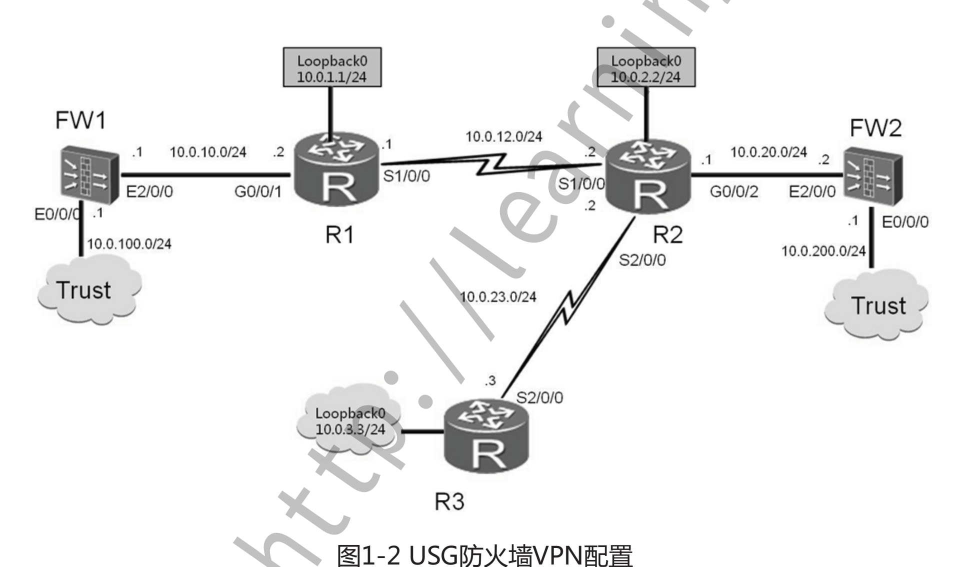


图1-2 USG防火墙VPN配置

场景

你是你们公司的网络管理员。公司的网络分为总部区域、分部网络和分支办公室三个部分。现在分部网络内Trust区域的用户需要能够访问总部的Trust区域。并且分支办公室也需要能够访问总部的Trust区域。并要求总部、分部网络之间，总部、分支办公室之间传输的数据需要加密。

学习任务

步骤一. 基本配置与 IP 编址

S1与S2参与到本次实验（实现防火墙与路由器的互联），但无需配置。实验之前，请清空S1与S2的配置，并重启它们。

给所有路由器配置IP地址和掩码。配置时注意所有的Loopback接口配置掩码均为24位。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.10.2 24
[R1-GigabitEthernet0/0/1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 24
[R1-Serial1/0/0]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.20.1 24
[R2-GigabitEthernet0/0/2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 24
[R2-Serial1/0/0]interface Serial2/0/0
[R2-Serial2/0/0]ip address 10.0.23.2 24
[R2-Serial2/0/0]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface Serial2/0/0
[R3-Serial2/0/0]ip address 10.0.23.3 24
[R3-Serial2/0/0]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24
```

配置防火墙FW1和FW2的接口地址。

```
<USG2100>system-view
```

```
Enter system view, return user view with Ctrl+Z.
[USG2100]sysname FW1
[FW1]interface Ethernet 0/0/0
[FW1-Ethernet0/0/0]ip address 10.0.100.1 24
[FW1-Ethernet0/0/0]interface Ethernet 2/0/0
[FW1-Ethernet2/0/0]ip address 10.0.10.1 24
[FW1-Ethernet2/0/0]interface vlanif 1
[FW1-Vlanif1]undo ip address

<USG2100>system-view
Enter system view, return user view with Ctrl+Z.
[USG2100]sysname FW2
[FW2]interface Ethernet 0/0/0
[FW2-Ethernet0/0/0]ip address 10.0.200.1 24
[FW2-Ethernet0/0/0]interface Ethernet 2/0/0
[FW2-Ethernet2/0/0]ip address 10.0.20.2 24
[FW2-Ethernet2/0/0]interface vlanif 1
[FW2-Vlanif1]undo ip address
```

配置防火墙FW1和FW2的安全区域，并将接口添加到对应的安全区域。

```
[FW1]firewall zone untrust
[FW1-zone-untrust]add interface Ethernet 2/0/0
[FW1-zone-untrust]undo add interface Ethernet0/0/0
[FW1-zone-untrust]quit
[FW1]firewall zone trust
[FW1-zone-trust]add interface Ethernet 0/0/0

[FW2]firewall zone untrust
[FW2-zone-untrust]add interface Ethernet 2/0/0
[FW2-zone-untrust]undo add interface Ethernet0/0/0
[FW2-zone-untrust]quit
[FW2]firewall zone trust
[FW2-zone-trust]add interface Ethernet 0/0/0
```

步骤二. 配置区域间的安全过滤

在防火墙上配置从Trust区域发往Untrust区域的数据包被放行，从Untrust区域发往Local区域的数据包被放行，其他方向数据流被禁止。

```
[FW1]firewall packet-filter default permit interzone trust untrust
[FW1]firewall packet-filter default permit interzone local untrust
```

```
[FW2]firewall packet-filter default permit interzone trust untrust
[FW2]firewall packet-filter default permit interzone local untrust
```

步骤三. 配置路由，实现网络的连通

在R1、R2、R3、FW1和FW2上配置单区域OSPF,实现10.0.10.0/24、10.0.20.0/24、10.0.12.0/24、10.0.23.0/24网段之间可以连通。

```
[R1]ospf 1
[R1-ospf-1]area 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.0.10.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255

[R2]ospf 1
[R2-ospf-1]area 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.20.0 0.0.0.255

[R3]ospf 1
[R3-ospf-1]area 0.0.0.0
[R3-ospf-1-area-0.0.0.0]network 10.0.23.0 0.0.0.255

[FW1]ospf 1
[FW1-ospf-1]area 0.0.0.0
[FW1-ospf-1-area-0.0.0.0]network 10.0.10.0 0.0.0.255

[FW2]ospf 1
[FW2-ospf-1]area 0.0.0.0
[FW2-ospf-1-area-0.0.0.0]network 10.0.20.0 0.0.0.255
```

在FW1和FW2上测试网段的连通性。

```
[FW1]ping 10.0.20.2
  PING 10.0.20.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.20.2: bytes=56 Sequence=1 ttl=253 time=40 ms
    Reply from 10.0.20.2: bytes=56 Sequence=2 ttl=253 time=30 ms
    Reply from 10.0.20.2: bytes=56 Sequence=3 ttl=253 time=30 ms
    Reply from 10.0.20.2: bytes=56 Sequence=4 ttl=253 time=40 ms
    Reply from 10.0.20.2: bytes=56 Sequence=5 ttl=253 time=30 ms
  --- 10.0.20.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
    0.00% packet loss
    round-trip min/avg/max = 30/34/40 ms
[FW1]ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=253 time=70 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=253 time=60 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=253 time=70 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=253 time=70 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=253 time=60 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/66/70 ms

[FW2]ping 10.0.10.1
  PING 10.0.10.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.1: bytes=56 Sequence=1 ttl=253 time=40 ms
    Reply from 10.0.10.1: bytes=56 Sequence=2 ttl=253 time=30 ms
    Reply from 10.0.10.1: bytes=56 Sequence=3 ttl=253 time=40 ms
    Reply from 10.0.10.1: bytes=56 Sequence=4 ttl=253 time=30 ms
    Reply from 10.0.10.1: bytes=56 Sequence=5 ttl=253 time=30 ms
  --- 10.0.10.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/34/40 ms
[FW2]ping 10.0.23.3
  PING 10.0.23.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.23.3: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 10.0.23.3: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 10.0.23.3: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 10.0.23.3: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.0.23.3: bytes=56 Sequence=5 ttl=254 time=30 ms
  --- 10.0.23.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/30/30 ms
```

R1、R2、R3、FW1和FW2连接的10.0.10.0/24、10.0.20.0/24、10.0.12.0/24、10.0.23.0/24网段之间可以连通。

步骤四. 配置分部网络与总部网络之间的 IPSec VPN

配置匹配被保护数据的ACL。

```
[FW1]acl 3000
[FW1-acl-adv-3000]rule permit ip source 10.0.100.0 0.0.0.255 destination 10.0.200.0 0.0.0.255

[FW2]acl 3000
[FW2-acl-adv-3000]rule permit ip source 10.0.200.0 0.0.0.255 destination 10.0.100.0 0.0.0.255
```

配置分部网络到总部内网的静态路由。

```
[FW1]ip route-static 10.0.200.0 24 10.0.10.2

[FW2]ip route-static 10.0.100.0 24 10.0.20.1
```

在防火墙FW1和FW2上配置IPSec安全提议。

配置时，封装模式使用隧道模式，使用ESP协议对数据进行保护。ESP使用的加密算法为DES、完整性验证算法使用SHA1。

```
[FW1]ipsec proposal tran1
[FW1-ipsec-proposal-tran1]encapsulation-mode tunnel
[FW1-ipsec-proposal-tran1]transform esp
[FW1-ipsec-proposal-tran1]esp authentication-algorithm sha1
[FW1-ipsec-proposal-tran1]esp encryption-algorithm des

[FW2]ipsec proposal tran1
[FW2-ipsec-proposal-tran1]encapsulation-mode tunnel
[FW2-ipsec-proposal-tran1]transform esp
[FW2-ipsec-proposal-tran1]esp authentication-algorithm sha1
[FW2-ipsec-proposal-tran1]esp encryption-algorithm des
```

在防火墙FW1和FW2上配置IKE安全提议。

在IKE安全提议中，定义加密算法为DES、完整性验证算法使用SHA1。

```
[FW1]ike proposal 10
[FW1-ike-proposal-10]authentication-algorithm sha1
[FW1-ike-proposal-10]encryption-algorithm des

[FW2]ike proposal 10
[FW2-ike-proposal-10]authentication-algorithm sha1
```

```
[FW2-ike-proposal-10]encryption-algorithm des
```

配置IKE对等体，IKE对等体默认使用IKEV2协商方式。

引用IKE安全提议，并定义对端IP地址和预共享密码。

```
[FW1]ike peer fw12
[FW1-ike-peer-fw12]ike-proposal 10
[FW1-ike-peer-fw12]remote-address 10.0.20.2
[FW1-ike-peer-fw12]pre-shared-key abcde

[FW2]ike peer fw21
[FW2-ike-peer-fw21]ike-proposal 10
[FW2-ike-peer-fw21]remote-address 10.0.10.1
[FW2-ike-peer-fw21]pre-shared-key abcde
```

在防火墙FW1和FW2上配置安全策略。

配置安全策略时，将ACL、IPSec安全提议及IKE对等体绑定在一块。

```
[FW1]ipsec policy map1 10 isakmp
[FW1-ipsec-policy-isakmp-map1-10]security acl 3000
[FW1-ipsec-policy-isakmp-map1-10]proposal tran1
[FW1-ipsec-policy-isakmp-map1-10]ike-peer fw12

[FW2]ipsec policy map1 10 isakmp
[FW2-ipsec-policy-isakmp-map1-10]security acl 3000
[FW2-ipsec-policy-isakmp-map1-10]proposal tran1
[FW2-ipsec-policy-isakmp-map1-10]ike-peer fw21
```

在防火墙FW1和FW2接口上应用安全策略。

```
[FW1]interface Ethernet2/0/0
[FW1-Ethernet2/0/0]ipsec policy map1

[FW2]interface Ethernet2/0/0
[FW2-Ethernet2/0/0]ipsec policy map1
```

测试分部网络内网到总部内网的连通性，然后查看IPSec建立情况。

```
[FW1]ping -a 10.0.100.1 10.0.200.1
 PING 10.0.200.1: 56  data bytes, press CTRL_C to break
   Reply from 10.0.200.1: bytes=56 Sequence=1 ttl=255 time=50 ms
   Reply from 10.0.200.1: bytes=56 Sequence=2 ttl=255 time=50 ms
   Reply from 10.0.200.1: bytes=56 Sequence=3 ttl=255 time=60 ms
   Reply from 10.0.200.1: bytes=56 Sequence=4 ttl=255 time=50 ms
```

```
  Reply from 10.0.200.1: bytes=56 Sequence=5 ttl=255 time=50 ms
 --- 10.0.200.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 50/52/60 ms
[FW1]display ike sa
current ike sa number: 2
-----------------------------------------------------------------------------
conn-id   peer                  flag         phase vpn
-----------------------------------------------------------------------------
40001     10.0.20.2              RD|ST         v2:2  public
1         10.0.20.2              RD|ST         v2:1  public

 flag meaning
 RD--READY   ST--STAYALIVE  RL--REPLACED     FD--FADING
 TO--TIMEOUT  TD--DELETING   NEG--NEGOTIATING  D--DPD
[FW1]display ipsec sa
===============================
Interface: Ethernet2/0/0
  path MTU: 1500
===============================
 -----------------------------
 IPsec policy name: "map1"
 sequence number: 10
 mode: isakmp
 vpn: public
 -----------------------------
  connection id: 40001
  rule number: 5
  encapsulation mode: tunnel
  holding time: 0d 0h 1m 16s
  tunnel local : 10.0.10.1    tunnel remote: 10.0.20.2
  flow      source: 10.0.100.0-10.0.100.255 0-65535 0
  flow destination: 10.0.200.0-10.0.200.255 0-65535 0

  [inbound ESP SAs]
   spi: 103447906 (0x62a7d62)
   vpn: public  said: 0  cpuid: 0x0000
   proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
   sa remaining key duration (bytes/sec): 1887436464/3524
   max received sequence-number: 4
   udp encapsulation used for nat traversal: N
```

```
[outbound ESP SAs]
  spi: 92831779 (0x5888023)
  vpn: public  said: 1  cpuid: 0x0000
  proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
  sa remaining key duration (bytes/sec): 1887436464/3524
  max sent sequence-number: 5
  udp encapsulation used for nat traversal: N
```

FW1连接的内网和FW2连接的内网可以通讯。

FW1和FW2之间已经建立两个方向的ESP SA。实现了分部网络和总部网络的数据通讯的加密。

步骤五. 配置分支办公室与总部之间的 IPSec VPN

配置分支办公室内网访问总部内网的ACL。

```
[R3]acl 3000
[R3-acl-adv-3000]rule permit ip source 10.0.3.0 0.0.0.255 destination 10.0.200.0
0.0.0.255

[FW2]acl 3001
[FW2-acl-adv-3001]rule permit ip source 10.0.200.0 0.0.0.255 destination
10.0.3.0 0.0.0.255
```

配置分支办公室到总部内网的静态路由。

```
[R3]ip route-static 10.0.200.0 24 10.0.23.2

[FW2]ip route-static 10.0.3.0 24 10.0.20.1
```

在R3上配置IPSec安全提议。

配置时，封装模式使用隧道模式，使用ESP协议对数据进行保护。ESP使用的加密算法为DES、完整性验证算法使用SHA1。

```
[R3]ipsec proposal tran1
[R3-ipsec-proposal-tran1]encapsulation-mode tunnel
[R3-ipsec-proposal-tran1]transform esp
[R3-ipsec-proposal-tran1]esp authentication-algorithm sha1
[R3-ipsec-proposal-tran1]esp encryption-algorithm des
```

在FW2和R3上配置IKE安全提议。

在IKE安全提议中，定义加密算法为DES、完整性验证算法使用SHA1。

```
[R3]ike proposal 10
[R3-ike-proposal-10]authentication-algorithm sha1
[R3-ike-proposal-10]encryption-algorithm des
```

配置IKE peer。IKE对等体使用IKEv2协商方式。

配置IKE对等体，引用IKE安全提议，并定义对端IP地址和预共享密码。

```
[FW2]ike peer fw23
[FW2-ike-peer-fw23]ike-proposal 10
[FW2-ike-peer-fw23]remote-address 10.0.23.3
[FW2-ike-peer-fw23]pre-shared-key abcde

[R3]ike peer r32 v2
[R3-ike-peer-r32]ike-proposal 10
[R3-ike-peer-r32]remote-address 10.0.20.2
[R3-ike-peer-r32]pre-shared-key abcde
```

在FW2和R3上配置安全策略。

配置安全策略时，将ACL、IPSec安全提议及IKE对等体绑定在一块。

```
[FW2]ipsec policy map1 11 isakmp
[FW2-ipsec-policy-isakmp-map1-11]security acl 3001
[FW2-ipsec-policy-isakmp-map1-11]proposal tran1
[FW2-ipsec-policy-isakmp-map1-11]ike-peer fw23

[R3]ipsec policy map1 10 isakmp
[R3-ipsec-policy-isakmp-map2-10]security acl 3000
[R3-ipsec-policy-isakmp-map2-10]proposal tran1
[R3-ipsec-policy-isakmp-map2-10]ike-peer r32
```

在FW2和R3上接口上应用安全策略。

```
[FW2]interface Ethernet2/0/0
[FW2-Ethernet2/0/0]ipsec policy map1

[R3]interface Serial2/0/0
[R3-Serial2/0/0]ipsec policy map1
```

测试分支办公室内网到总部内网的连通性，然后查看IPSec建立情况。

查看已经建立起来的IKE SA时，需要在命令中使用v2参数。

```
[R3]ping -a 10.0.3.3 10.0.200.1
```

```
  PING 10.0.200.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.200.1: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 10.0.200.1: bytes=56 Sequence=2 ttl=255 time=48 ms
    Reply from 10.0.200.1: bytes=56 Sequence=3 ttl=255 time=48 ms
    Reply from 10.0.200.1: bytes=56 Sequence=4 ttl=255 time=48 ms
    Reply from 10.0.200.1: bytes=56 Sequence=5 ttl=255 time=48 ms
  --- 10.0.200.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 48/48/50 ms
[R3]display ike sa v2
    Conn-ID  Peer           VPN   Flag(s)              Phase
  ---------------------------------------------------------------
      2    10.0.20.2       0     RD|ST                      2
      1    10.0.20.2       0     RD|ST                      1
  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
[R3]display ipsec sa
===============================
Interface: Serial2/0/0
 Path MTU: 1500
===============================
  -----------------------------
  IPSec policy name: "map1"
  Sequence number  : 10
  Mode             : ISAKMP
  -----------------------------
    Connection ID     : 2
    Encapsulation mode: Tunnel
    Tunnel local      : 10.0.23.3
    Tunnel remote     : 10.0.20.2
    [Outbound ESP SAs]
      SPI: 247406703 (0xebf206f)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436380/3534
      Max sent sequence-number: 5
      UDP encapsulation used for NAT traversal: N
    [Inbound ESP SAs]
      SPI: 155207494 (0x9404746)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436380/3534
```

```
Max received sequence-number: 5
UDP encapsulation used for NAT traversal: N
```

FW2连接的内网和R3连接的内网可以通讯。

FW2和R3之间已经建立IPSec VPN通道。实现了分支办公室网络和总部网络的数据通讯的加密。

步骤六. 配置分部网络与总部之间的 GRE over IPSec VPN

以上步骤中，通过配置静态路由，实现了三个内网之间的通讯。

随着网络规模的增大，配置静态路由得复杂性会增大，需要使用动态路由协议实现网络之间的互通。

动态路由协议不支持在IPSec通道上运行。

可以通过使用GRE Over IPSec技术来支持动态路由协议，实现三个内网之间的的通讯。

FW1上创建Tunnel接口，隧道采用GRE协议。

将Tunnel接口添加到FW1的Untrust区域。

```
[FW1]interface tunnel 1
[FW1-Tunnel1]tunnel-protocol gre
[FW1-Tunnel1]ip address 30.1.1.1 24
[FW1-Tunnel1]source 10.0.10.1
[FW1-Tunnel1]destination 10.0.20.2
[FW1-Tunnel1]firewall zone untrust
[FW1-zone-untrust]add interface Tunnel 1
```

FW2上创建Tunnel接口，隧道采用GRE协议。

将Tunnel接口添加到FW2的Untrust区域。

```
[FW2]interface tunnel 1
[FW2-Tunnel1]tunnel-protocol gre
[FW2-Tunnel1]ip address 30.1.1.2 24
[FW2-Tunnel1]source 10.0.20.2
[FW2-Tunnel1]destination 10.0.10.1
[FW2-Tunnel1]firewall zone untrust
[FW2-zone-untrust]add interface Tunnel 1
```

删除以上步骤配置的静态路由，在分部网络和总部内网之间配置使用RIP路由协议。RIP协议使用版本2。

```
[FW1]undo ip route-static 10.0.200.0 24 10.0.10.2
[FW1]rip
[FW1-rip-1]version 2
[FW1-rip-1]network 30.0.0.0
[FW1-rip-1]network 10.0.0.0

[FW2]undo ip route-static 10.0.100.0 24 10.0.20.1
[FW2]rip
[FW2-rip-1]version 2
[FW2-rip-1]network 30.0.0.0
[FW2-rip-1]network 10.0.0.0
```

配置ACL，定义GRE封装之后的数据为需要被IPSec加密的数据流。

配置安全策略，绑定新定义的ACL。

```
[FW1]acl 3001
[FW1-acl-adv-3001]rule permit gre source 10.0.10.1 0 destination 10.0.20.2 0
[FW1-acl-adv-3001]quit
[FW1]ipsec policy map1 10 isakmp
[FW1-ipsec-policy-isakmp-map1-10]security acl 3001

[FW2]acl 3002
[FW2-acl-adv-3002]rule permit gre source 10.0.20.2 0 destination 10.0.10.1 0
[FW2-acl-adv-3002]quit
[FW2]ipsec policy map1 10 isakmp
[FW2-ipsec-policy-isakmp-map1-10]security acl 3002
```

其他配置保持不变。

测试分部网络内网到总部内网的连通性，查看IPSec建立情况。

```
[FW1]ping -a 10.0.100.1 10.0.200.1
 PING 10.0.200.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.200.1: bytes=56 Sequence=1 ttl=255 time=50 ms
    Reply from 10.0.200.1: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.0.200.1: bytes=56 Sequence=3 ttl=255 time=60 ms
    Reply from 10.0.200.1: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 10.0.200.1: bytes=56 Sequence=5 ttl=255 time=50 ms
  --- 10.0.200.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/52/60 ms
[FW1]display ipsec sa
```

```
================================
Interface: Ethernet2/0/0
   path MTU: 1500
================================
  -----------------------------
  IPsec policy name: "map1"
  sequence number: 10
  mode: isakmp
  vpn: public
  -----------------------------
    connection id: 40003
    rule number: 5
    encapsulation mode: tunnel
    holding time: 0d 0h 5m 21s
    tunnel local : 10.0.10.1    tunnel remote: 10.0.20.2
    flow      source: 10.0.100.0-10.0.100.255 0-65535 0
    flow destination: 10.0.200.0-10.0.200.255 0-65535 0
    [inbound ESP SAs]
      spi: 240396810 (0xe542a0a)
      vpn: 0     said: 34  cpuid: 0x0000
      proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      sa remaining key duration (bytes/sec): 1887436044/3279
      max received sequence-number: 9
      udp encapsulation used for nat traversal: N
    [outbound ESP SAs]
      spi: 208723708 (0xc70defc)
      vpn: 0     said: 35  cpuid: 0x0000
      proposal: ESP-ENCRYPT-DES ESP-AUTH-SHA1
      sa remaining key duration (bytes/sec): 1887436044/3279
      max sent sequence-number: 10
      udp encapsulation used for nat traversal: N
```

分部网络内网到总部内网可以连通。

FW1和FW2已经建立GRE over IPSec VPN通道。实现了RIP路由信息在分部网络和总部网络的传递。

步骤七. 配置分支办公室与总部之间的 GRE over IPSec VPN

FW2上创建Tunnel接口，隧道采用GRE协议。

将Tunnel接口添加到FW2的Untrust区域。

```
[FW2]interface tunnel 2
```

```
[FW2-Tunnel2]tunnel-protocol gre
[FW2-Tunnel2]ip address 40.1.1.1 24
[FW2-Tunnel2]source 10.0.20.2
[FW2-Tunnel2]destination 10.0.23.3
[FW2-Tunnel2]firewall zone untrust
[FW2-zone-untrust]add interface Tunnel 2
```

R3上创建Tunnel接口，隧道采用GRE协议。

```
[R3]interface tunnel 0/0/1
[R3-Tunnel0/0/1]tunnel-protocol gre
[R3-Tunnel0/0/1]ip address 40.1.1.2 24
[R3-Tunnel0/0/1]source 10.0.23.3
[R3-Tunnel0/0/1]destination 10.0.20.2
```

删除以上步骤配置的静态路由，在分支办公室网络和总部内网之间配置使用RIP路由协议。RIP协议使用版本2。

```
[FW2]undo ip route-static 10.0.3.0 24 10.0.20.1
[FW2]rip
[FW2-rip-1]version 2
[FW2-rip-1]network 40.0.0.0

[R3]undo ip route-static 10.0.200.0 24 10.0.23.2
[R3]rip
[R3-rip-1]version 2
[R3-rip-1]network 40.0.0.0
[R3-rip-1]network 10.0.0.0
```

配置ACL定义GRE封装之后的数据为需要被IPSec加密的数据流。

配置安全策略，绑定新的ACL、IPSec安全提议及IKE对等体

```
[R3]acl 3001
[R3-acl-adv-3001]rule permit gre source 10.0.23.3 0 destination 10.0.20.2 0
[R3-acl-adv-3001]quit
[R3]ipsec policy map1 20 isakmp
[R3-ipsec-policy-isakmp-map1-10]security acl 3001
[R3-ipsec-policy-isakmp-map1-20]proposal tran1
[R3-ipsec-policy-isakmp-map1-20]ike-peer r32

[FW2]acl 3003
[FW2-acl-adv-3003]rule permit gre source 10.0.20.2 0 destination 10.0.23.3 0
[FW2-acl-adv-3003]quit
[FW2]ipsec policy map1 20 isakmp
```

```
[FW2-ipsec-policy-isakmp-map1-20]security acl 3003
[FW2-ipsec-policy-isakmp-map1-20]proposal tran1
[FW2-ipsec-policy-isakmp-map1-20]ike-peer fw23
```

其他配置保持不变。

测试分支办公室内网到总部内网的连通性，查看IPSec建立情况。

```
[R3]ping -a 10.0.3.3 10.0.200.1
  PING 10.0.200.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.200.1: bytes=56 Sequence=1 ttl=255 time=56 ms
    Reply from 10.0.200.1: bytes=56 Sequence=2 ttl=255 time=53 ms
    Reply from 10.0.200.1: bytes=56 Sequence=3 ttl=255 time=54 ms
    Reply from 10.0.200.1: bytes=56 Sequence=4 ttl=255 time=54 ms
    Reply from 10.0.200.1: bytes=56 Sequence=5 ttl=255 time=54 ms
  --- 10.0.200.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 53/54/56 ms
[R3]display ipsec sa
===============================
Interface: Serial2/0/0
 Path MTU: 1500
===============================

  -----------------------------
  IPSec policy name: "map1"
  Sequence number  : 10
  Mode             : ISAKMP
  -----------------------------
    Connection ID     : 2
    Encapsulation mode: Tunnel
    Tunnel local      : 10.0.23.3
    Tunnel remote     : 10.0.20.2

    [Outbound ESP SAs]
      SPI: 145201056 (0x8a797a0)
      Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436380/2849
      Max sent sequence-number: 5
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
```

```
    SPI: 1040062082 (0x3dfe1682)
    Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
    SA remaining key duration (bytes/sec): 1887436380/2849
    Max received sequence-number: 5
    UDP encapsulation used for NAT traversal: N

-----------------------------
IPSec policy name: "map1"
Sequence number  : 20
Mode             : ISAKMP
-----------------------------
  Connection ID     : 5
  Encapsulation mode: Tunnel
  Tunnel local      : 10.0.23.3
  Tunnel remote     : 10.0.20.2

  [Outbound ESP SAs]
    SPI: 97199512 (0x5cb2598)
    Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
    SA remaining key duration (bytes/sec): 1887436200/3506
    Max sent sequence-number: 6
    UDP encapsulation used for NAT traversal: N

  [Inbound ESP SAs]
    SPI: 2570078602 (0x9930498a)
    Proposal: ESP-ENCRYPT-DES-64 ESP-AUTH-SHA1
    SA remaining key duration (bytes/sec): 1887436176/3506
    Max received sequence-number: 5
    UDP encapsulation used for NAT traversal: N
```

分支办公室网络到总部内网可以连通。

FW2和R3之间已经建立GRE over IPSec VPN通道。实现了RIP信息在分支办公室网络和总部网络的传递。

附加实验：思考并验证

步骤五中配置分支办公室与总部之间的IPSec时，R3不使用IKEv2与FW2协商的话，IKE SA能建立吗？

最终设备配置

```
[FW1]display current-configuration
```

```
#
sysname FW1
#
acl number 3000
 rule 5 permit ip source 10.0.100.0 0.0.0.255 destination 10.0.200.0 0.0.0.255
#
acl number 3001
 rule 5 permit gre source 10.0.10.1 0 destination 10.0.20.2 0
#
ike proposal 10
#
ike peer fw12
 pre-shared-key abcde
 ike-proposal 10
 remote-address 10.0.20.2
#
ipsec proposal tran1
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 security acl 3001
 ike-peer fw12
 proposal tran1
#
interface Ethernet0/0/0
 ip address 10.0.100.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 10.0.10.1 255.255.255.0
 ipsec policy map1
#
interface Tunnel1
 ip address 30.1.1.1 255.255.255.0
 tunnel-protocol gre
 source 10.0.10.1
 destination 10.0.20.2
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet0/0/0
```

```
#
firewall zone untrust
 set priority 5
 add interface Ethernet2/0/0
 add interface Tunnel1
#
ospf 1
 area 0.0.0.0
  network 10.0.10.0 0.0.0.255
#
rip 1
 version 2
 network 30.0.0.0
 network 10.0.0.0
#
Return

[FW2]display current-configuration
#
sysname FW2
#
acl number 3000
 rule 5 permit ip source 10.0.200.0 0.0.0.255 destination 10.0.100.0 0.0.0.255
#
acl number 3001
 rule 5 permit ip source 10.0.200.0 0.0.0.255 destination 10.0.3.0 0.0.0.255
#
acl number 3002
 rule 5 permit gre source 10.0.20.2 0 destination 10.0.10.1 0
#
acl number 3003
 rule 5 permit gre source 10.0.20.2 0 destination 10.0.23.3 0
#
ike proposal 10
#
ike peer fw21
 pre-shared-key abcde
 ike-proposal 10
 remote-address 10.0.10.1
#
ike peer fw23
 pre-shared-key abcde
 ike-proposal 10
```

```
 remote-address 10.0.23.3
#
ipsec proposal tran1
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 security acl 3002
 ike-peer fw21
 proposal tran1
#
ipsec policy map1 11 isakmp
 security acl 3001
 ike-peer c
 proposal tran1
#
ipsec policy map1 20 isakmp
 security acl 3003
 ike-peer fw23
 proposal tran1
#
interface Ethernet0/0/0
 ip address 10.0.200.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 10.0.20.2 255.255.255.0
 ipsec policy map1
#
interface Tunnel1
 ip address 30.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.0.20.2
 destination 10.0.10.1
#
interface Tunnel2
 ip address 40.1.1.1 255.255.255.0
 tunnel-protocol gre
 source 10.0.20.2
 destination 10.0.23.3
#
firewall zone local
 set priority 100
#
firewall zone trust
```

```
 set priority 85
 add interface Ethernet0/0/0
#
firewall zone untrust
 set priority 5
 add interface Ethernet2/0/0
 add interface Tunnel1
 add interface Tunnel2
#
firewall zone dmz
 set priority 50
#
ospf 1
 area 0.0.0.0
  network 10.0.20.0 0.0.0.255
#
rip 1
 version 2
 network 30.0.0.0
 network 10.0.0.0
 network 40.0.0.0
#
Return

[R3]display current-configuration
[V200R001C00SPC200]
#
 sysname R3
#
acl number 3000
 rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.200.0 0.0.0.255
#
acl number 3001
 rule 5 permit gre source 10.0.23.3 0 destination 10.0.20.2 0
#
ipsec proposal tran1
 esp authentication-algorithm sha1
#
ike proposal 10
#
ike peer r32 v2
 pre-shared-key abcde
 ike-proposal 10
```

```
 remote-address 10.0.20.2
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer r32
 proposal tran1
#
ipsec policy map1 20 isakmp
 security acl 3001
 ike-peer r32
 proposal tran1
#
interface Serial2/0/0
 link-protocol ppp
 ip address 10.0.23.3 255.255.255.0
 ipsec policy map1
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
interface Tunnel0/0/1
 ip address 40.1.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.0.23.3
 destination 10.0.20.2
#
ospf 1
 area 0.0.0.0
  network 10.0.23.0 0.0.0.255
#
rip 1
 version 2
 network 40.0.0.0
 network 10.0.0.0
#
return
```

实验 1-3 防火墙攻击防范配置

学习目的

- 掌握防范流量型攻击的配置方法
- 掌握防范扫描窥探型攻击的配置方法
- 掌握防范畸形报文攻击的配置方法
- 掌握防范特殊报文攻击的配置方法

拓扑图

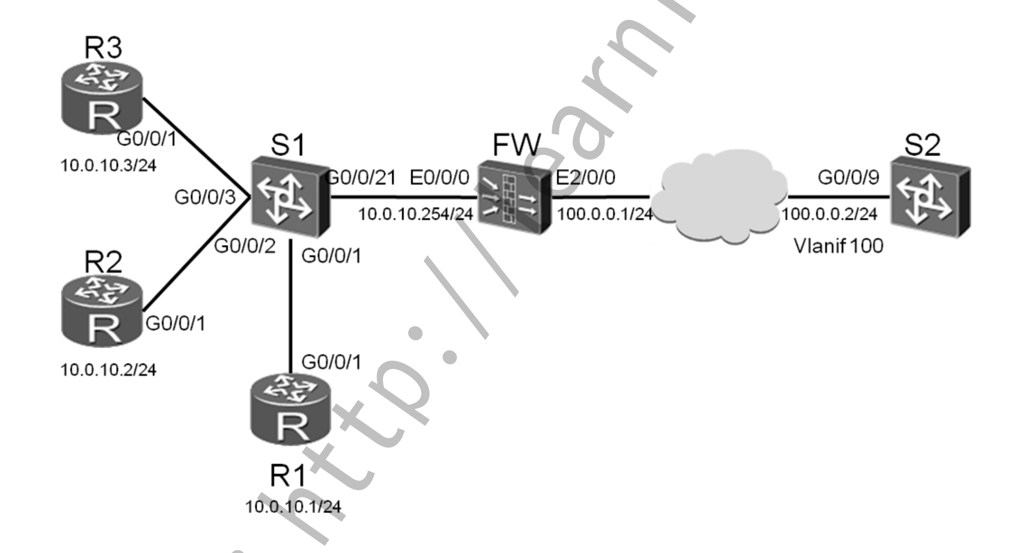


图1-3 防火墙攻击防范配置

场景

你是公司的网络管理员。现在公司网络是由一台防火墙和一台交换机组成，R1是公司的DHCP服务器，防火墙作为公司内网用户连接Internet的出口,S2模拟外网的计算机。

为了提高网络的安全性，需要在网络中应用安全策略。需要你通过在防火墙和交换机上配置各种安全策略实现对内外网的保护。

学习任务

步骤一. 基础配置与 IP 编址

给所有设备配置IP地址和掩码。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.10.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.10.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.10.3 24

<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
[Quidway]sysname S1

<USG2100>system-view
Enter system view, return user view with Ctrl+Z.
[USG2100]sysname FW
[FW]interface Ethernet 0/0/0
[FW-Ethernet0/0/0]ip address 10.0.10.254 24
[FW-Ethernet0/0/0]interface Ethernet 2/0/0
[FW-Ethernet2/0/0]ip address 100.0.0.1 24
[FW-Ethernet2/0/0]quit
[FW]firewall packet-filter default permit all
[FW]firewall zone untrust
[FW-zone-untrust]add interface Ethernet 2/0/0

<Quidway>system-view
Enter system view, return user view with Ctrl+Z.
```

```
[Quidway]sysname S2
[S2]vlan 100
[S2-vlan100]quit
[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]port link-type access
[S2-GigabitEthernet0/0/9]port default vlan 100
[S2-GigabitEthernet0/0/9]quit
[S2]interface Vlanif 100
[S2-Vlanif100]ip address 100.0.0.2 24

[S1]vlan 100
[S1-vlan100]quit
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]port link-type access
[S1-GigabitEthernet0/0/9]port default vlan 100
[S1-GigabitEthernet0/0/9]interface GigabitEthernet 0/0/23
[S1-GigabitEthernet0/0/23]port link-type access
[S1-GigabitEthernet0/0/23]port default vlan 100
```

关闭S1的G0/0/10、G0/0/13和G0/0/14接口，避免对实验造成影响。

```
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]shutdown
[S1-GigabitEthernet0/0/10]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]shutdown
[S1-GigabitEthernet0/0/13]interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14]shutdown
```

配置完成后，测试直连链路的连通性。

```
[R1]ping -c 1 10.0.10.2
  PING 10.0.10.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.2: bytes=56 Sequence=1 ttl=255 time=2 ms

  --- 10.0.10.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms

[R1]ping -c 1 10.0.10.3
  PING 10.0.10.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.3: bytes=56 Sequence=1 ttl=255 time=2 ms
```

```
  --- 10.0.10.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms

[R1]ping -c 1 10.0.10.254
  PING 10.0.10.254: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.254: bytes=56 Sequence=1 ttl=255 time=3 ms

  --- 10.0.10.254 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

[FW]ping -c 1 100.0.0.2
10:47:09  2011/12/27
  PING 100.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 100.0.0.2: bytes=56 Sequence=1 ttl=254 time=1 ms

  --- 100.0.0.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

步骤二. 实现网络互通

各模拟计算机的设备只需要正确配置网关即可以实现网络互通。

在R1、R2、R3和S2配置网关。

```
[R1]ip route-static 0.0.0.0 0 10.0.10.254

[R2]ip route-static 0.0.0.0 0 10.0.10.254

[R3]ip route-static 0.0.0.0 0 10.0.10.254

[S2]ip route-static 0.0.0.0 0 100.0.0.1
```

在S2上测试与R1、R2、R3的连通性。

```
[S2]ping -c 1 10.0.10.1
  PING 10.0.10.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.1: bytes=56 Sequence=1 ttl=254 time=1 ms

  --- 10.0.10.1 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[S2]ping -c 1 10.0.10.2
  PING 10.0.10.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.2: bytes=56 Sequence=1 ttl=254 time=1 ms

  --- 10.0.10.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[S2]ping -c 1 10.0.10.3
  PING 10.0.10.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.3: bytes=56 Sequence=1 ttl=254 time=1 ms

  --- 10.0.10.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

步骤三.　配置流量型攻击防范

攻击者可以发送大量的无用数据去占用过多的服务器资源。使服务器无法响应正常的服务请求，以达到服务器拒绝服务的目的。

针对这种攻击我们可以为设备配置SYN Flood防范、TCP全连接防范、HTTP Flood防范、UDP Flood防范和ICMP Flood防范这些方法保护网络。

在FW的E2/0/0接口上开启基于TCP反向源探测防范功能。

```
[FW]firewall source-ip detect interface Ethernet 2/0/0 alert-rate 10000 max-rate 30000
```

在FW上开启TCP全连接防范功能。

```
[FW]firewall blacklist enable
[FW]firewall session link-state check
[FW]firewall defend tcp-illegal-session enable
Warning: Configuring this command will affect the P2P service. To protect the
server from TCP connection exhaustion, configure this command.
Continue? [Y/N]:y
```

在FW的E2/0/0接口上开启HTTP Flood防范功能。

```
[FW]firewall defend http-flood enable
[FW]firewall defend http-flood source-detect interface Ethernet 2/0/0 alert-rate
10000 max-rate 30000
```

在FW的E2/0/0接口上开启UDP Flood防范功能。

```
[FW]firewall defend udp-flood enable
[FW]firewall defend udp-flood interface Ethernet2/0/0 max-rate 20000
```

在FW的E2/0/0接口上开启ICMP Flood防范功能。

```
[FW]firewall defend icmp-flood enable
[FW]firewall defend icmp-flood interface Ethernet 2/0/0 max-rate 10000
```

步骤四. 配置扫描窥探型攻击防范

攻击者发送目的端口不断变化的数据包来了解目的提供的服务种类和潜在安全漏洞。针对这种窥探我们可以为设备配置端口扫描攻击防范功能来保护网络。

在FW上开启端口扫描攻击防范功能。

```
[FW]firewall defend port-scan enable
[FW]firewall defend port-scan max-rate 5000
```

步骤五. 配置畸形报文攻击防范

攻击者如果向系统发送有缺陷的IP报文，就有可能使目标系统在处理这些报文时出错，从而达到影响目标系统正常运行的目的。一个安全的网络需要保障用户系统的正常运行，针对这种攻击可以为设备配置Smurf攻击防范、Land攻击防范、Fraggle攻击防范等等。同时在接入层网络上通过部署DHCP Snooping等安全措施整体提升网络安全。

在FW上开启Smurf攻击防范功能。

```
[FW]firewall defend smurf enable
```

在FW上开启Land攻击防范功能。

```
[FW]firewall defend land enable
```

在FW上开启Fraggle攻击防范功能。

```
[FW]firewall defend fraggle enable
```

在FW上开启IP分片报文攻击防范功能。

```
[FW]firewall defend ip-fragment enable
```

在FW上开启TCP报文标志位攻击防范功能。

```
[FW]firewall defend tcp-flag enable
```

将R1配置为DHCP服务器。

```
[R1]dhcp enable
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]dhcp select global
[R1-GigabitEthernet0/0/1]quit
[R1]ip pool company
[R1-ip-pool-company]network 10.0.10.0 mask 24
[R1-ip-pool-company]excluded-ip-address 10.0.10.1
[R1-ip-pool-company]gateway-list 10.0.10.254
```

将R2和R3的G0/0/1接口配置为自动获取IP地址。

```
[R2]dhcp enable
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]undo ip address
[R2-GigabitEthernet0/0/1]ip address dhcp-alloc
Info: The operation may take a few seconds, please wait.
Succeed.

[R3]dhcp enable
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]undo ip address
[R3-GigabitEthernet0/0/1]ip address dhcp-alloc
Info: The operation may take a few seconds, please wait.
Succeed.
```

在S1上开启DHCP Snooping功能，并为接口配置信任关系。

```
[S1]dhcp enable
[S1]dhcp snooping enable
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]dhcp snooping trusted
[S1-GigabitEthernet0/0/1]inter GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]dhcp snooping enable
[S1-GigabitEthernet0/0/2]inter GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]dhcp snooping enable
```

查看R1的G0/0/1接口MAC地址和FW的E0/0/0接口MAC地址，并配置静态用户绑定。

```
[R1]display interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-12-27 10:21:41
Description:HUAWEI, AR Series, GigabitEthernet0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.0.10.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 5489-9876-81f0
Last physical up time   : 2011-12-27 10:14:07
Last physical down time : 2011-12-27 10:13:48
Current system time: 2011-12-27 16:24:49
Port Mode: COMMON COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO
Last 300 seconds input rate 704 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 7392 bits/sec,Record time: 2011-12-27 10:17:53
Output peak rate 2816 bits/sec,Record time: 2011-12-27 10:17:13

Input:  12040 packets, 1641163 bytes
  Unicast:              0,  Multicast:               0
  Broadcast:            0,  Jumbo:                   0
  Discard:              0,  Total Error:             0
……output omit……

[FW]display interface Ethernet 0/0/0
Ethernet0/0/0 current state : UP
Line protocol current state : UP
Description : Huawei, usg2160 serials, Ethernet0/0/0 Interface, Route Port
```

```
The Maximum Transmit Unit is 1500 bytes, Hold timer is 10(sec)
Internet Address is 10.0.10.254/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0022-a109-68b2
Media type is twisted pair, loopback not set, promiscuous mode not set
100Mb/s-speed mode, Full-duplex mode, link type is auto negotiation
Output flow-control is unsupported, input flow-control is unsupported
QoS max-bandwidth : 100000 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Frag queue : Size/Length/Discards)  0/1000/0
Output queue : (Protocol queue : Size/Length/Discards) 0/1000/0
Output queue : (FIFO queue : Size/Length/Discards)  0/256/0
   Last 300 seconds input rate 59.50 bytes/sec, 0.50 packets/sec
   Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
   Input: 11778 packets, 1527521 bytes
         478 broadcasts(4.06%), 11230 multicasts(95.35%)
         0 runts, 0 giants,
         0 errors, 0 CRC,
         0 collisions, 0 late collisions, 0 overruns,
         0 jabbers, 0 input no buffers, 0 Resource errors,
         0 other errors
……output omit……

[S1]user-bind static ip-address 10.0.10.1 mac-address 5489-9876-81f0
[S1]user-bind static ip-address 10.0.10.254 mac-address 0022-a109-68b2
```

开启IP源防攻击功能。

```
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]ip source check user-bind enable
Info: Add permit rule for dynamic snooping bind-table, please wait a minute!
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]ip source check user-bind enable
Info: Add permit rule for dynamic snooping bind-table, please wait a minute!
```

配置IP报文检查选项。

```
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]ip source check user-bind check-item ip-address
mac-address
Info: Change permit rule for dynamic snooping bind-table, please wait a minute!
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]ip source check user-bind check-item ip-address
mac-address
Info: Change permit rule for dynamic snooping bind-table, please wait a minute!
```

配置ARP报文源MAC地址检查功能。

```
[S1]arp anti-attack packet-check sender-mac
```

配置防止ARP中间人攻击。

```
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]arp anti-attack check user-bind enable
[S1-GigabitEthernet0/0/2]arp anti-attack check user-bind check-item ip-address
mac-address
 Info: Change permit rule for dynamic dhcp snooping bind-table, please wait a
minute!
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]arp anti-attack check user-bind enable
[S1-GigabitEthernet0/0/3]arp anti-attack check user-bind check-item ip-address
mac-address
 Info: Change permit rule for dynamic dhcp snooping bind-table, please wait a
minute!
```

步骤六.　配置特殊报文攻击防御

攻击者可以利用一些很少用到的合法报文对网络进行侦察。针对这种攻击可以为设备配置超大ICMP攻击防范、ICMP重定向报文攻击防范、ICMP不可达报文攻击防范等等功能提升网络安全性。

在FW上开启超大ICMP报文攻击防范功能。

```
[FW]firewall defend large-icmp enable
[FW]firewall defend large-icmp max-length 3000
```

在FW上开启ICMP重定向报文攻击防范功能。

```
[FW]firewall defend icmp-redirect enable
```

在FW上开启ICMP不可达报文攻击防范功能。

```
[FW]firewall defend icmp-unreachable enable
```

在FW上开启带路由记录项的IP报文攻击防范功能。

```
[FW]firewall defend route-record enable
```

在FW上配置带源路由选项的IP报文攻击防范功能。

```
[FW]firewall defend source-route enable
```

在FW上配置Tracert报文攻击防范功能。

```
[FW]firewall defend tracert enable
```

在FW上配置带时间戳选项的IP报文攻击防范功能。

```
[FW]firewall defend time-stamp enable
```

附加实验：思考并验证

在实际的网络中，防火墙能起到的作用往往很有限，往往我们需要IPS设备进行另外一个层面的攻击防范。

请搜索关于IPS的相关知识，并对比它与防火墙的差异。

最终设备配置

```
[FW]display current-configuration
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit interzone local untrust direction inbound
 firewall packet-filter default permit interzone local untrust direction outbound
 firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outbound
 firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
#
 firewall defend tcp-illegal-session enable
 firewall defend http-flood enable
 firewall defend port-scan enable
 firewall defend time-stamp enable
 firewall defend route-record enable
 firewall defend source-route enable
 firewall defend ip-fragment enable
 firewall defend tcp-flag enable
 firewall defend fraggle enable
```

```
 firewall defend tracert enable
 firewall defend icmp-unreachable enable
 firewall defend icmp-redirect enable
 firewall defend large-icmp enable
 firewall defend icmp-flood enable
 firewall defend udp-flood enable
 firewall defend smurf enable
 firewall defend land enable
 firewall defend port-scan max-rate 5000
 firewall defend large-icmp max-length 3000
 firewall defend http-flood source-detect interface Ethernet2/0/0 alert-rate
10000 max-rate 30000
 firewall source-ip detect interface Ethernet2/0/0 alert-rate 10000 max-rate
30000
 firewall defend icmp-flood interface Ethernet2/0/0 max-rate 10000
 firewall defend udp-flood interface Ethernet2/0/0 max-rate 20000
#
interface Ethernet0/0/0
 ip address 10.0.10.254 255.255.255.0
#
interface Ethernet2/0/0
 ip address 100.0.0.1 255.255.255.0
#
interface NULL0
#
firewall zone untrust
 set priority 5
 add interface Ethernet0/0/0
 add interface Ethernet2/0/0
#
firewall zone dmz
 set priority 50
#
 firewall blacklist enable
#
return

[S1]display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S1
#
 vlan batch 100
```

```
#
 dhcp enable
 dhcp snooping enable
 user-bind static ip-address 10.0.10.1 mac-address 5489-9876-81f0
 user-bind static ip-address 10.0.10.254 mac-address 0022-a109-68b2
#
interface GigabitEthernet0/0/1
 dhcp snooping trusted
#
interface GigabitEthernet0/0/2
 dhcp snooping enable
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address mac-address
 ip source check user-bind enable
 ip source check user-bind check-item ip-address mac-address
#
interface GigabitEthernet0/0/3
 dhcp snooping enable
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address mac-address
 ip source check user-bind enable
 ip source check user-bind check-item ip-address mac-address
#
interface GigabitEthernet0/0/9
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/10
 shutdown
#
interface GigabitEthernet0/0/13
 shutdown
#
interface GigabitEthernet0/0/14
 shutdown
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/24
#
return
```

实验 1-4USG 防火墙 NAT 配置

学习目的

- 掌握在USG防火墙上配置NAT Easy IP的方法
- 掌握在USG防火墙上基于地址池配置NAPT的方法
- 掌握在USG防火墙上配置NAT Server的方法
- 掌握在USG防火墙上配置域内NAT Server的方法

拓扑图

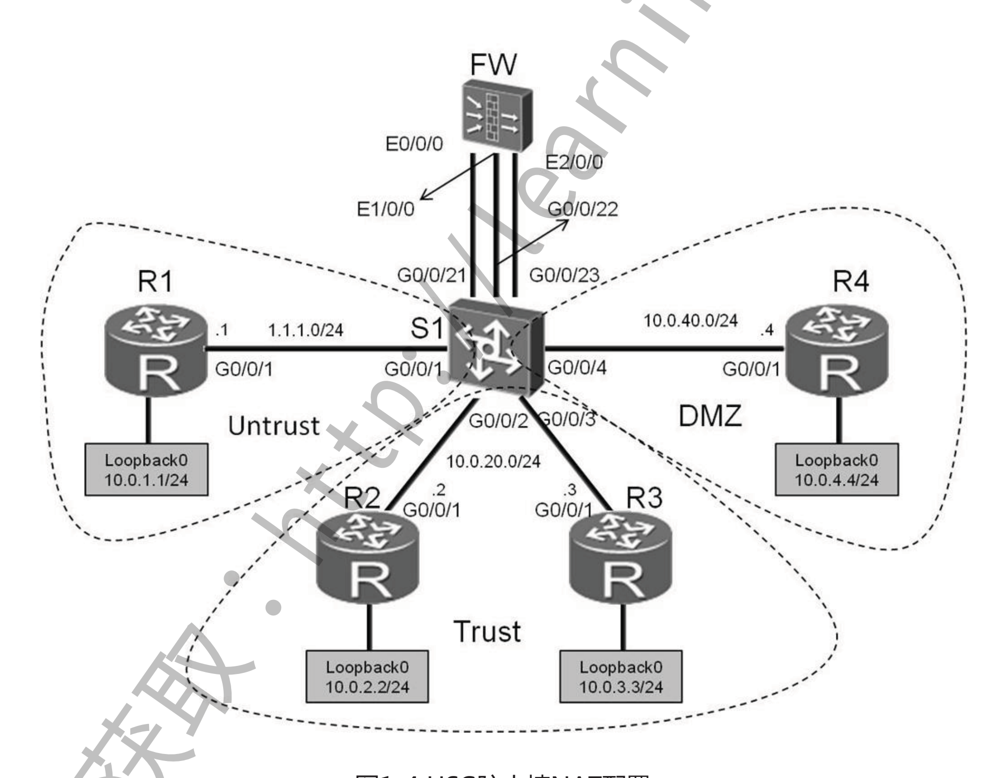


图1-4 USG防火墙NAT配置

场景

你是你们公司的网络管理员。公司的网络使用防火墙隔离成三个区域。现在

内部网络Trust区域的用户需要能够访问外部区域。并且需要将DMZ区域中的一台服务器（IP地址为10.0.4.4）提供的Telnet服务和FTP服务发布出去，对外公开的地址为1.1.1.100/24。

此外，还需要将内部网络一台服务器10.0.3.3提供的Telnet服务发布出去，使Trust区域的用户能够使用1.1.1.200/24访问。其他方向的访问被禁止。

学习任务

步骤一. 基本配置与 IP 编址

给所有路由器配置IP地址和掩码。配置时注意所有的Loopback接口配置掩码均为24位。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 1.1.1.1 24
[R1-GigabitEthernet0/0/1]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.20.2 24
[R2-GigabitEthernet0/0/1]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.20.3 24
[R3-GigabitEthernet0/0/1]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.40.4 24
```

```
[R4-GigabitEthernet0/0/1]interface loopback 0
[R4-LoopBack0]ip address 10.0.4.4 24
```

给防火墙配置地址时，需要注意Ethernet1/0/0接口为二层交换机接口，无法配置IP地址。实验中我们在防火墙上配置VLAN12，定义Vlanif12。配置IP地址作为Inside区域的网关，使用IP地址10.0.20.254/24。

默认情况下防火墙会给它的Vlanif1配置地址，实验中为避免干扰，删除该配置。

```
<USG2100>system-view
Enter system view, return user view with Ctrl+Z.
[USG2100]sysname FW
[FW]vlan 12
[FW-vlan-12]quit
[FW]interface Vlanif 12
[FW-Vlanif12]ip address 10.0.20.254 24
[FW-Vlanif12]interface ethernet 1/0/0
[FW-Ethernet1/0/0]port  access vlan 12
[FW-Ethernet1/0/0]interface Ethernet 0/0/0
[FW-Ethernet0/0/0]ip address 1.1.1.254 24
[FW-Ethernet0/0/0]interface ethernet 2/0/0
[FW-Ethernet2/0/0]ip address 10.0.40.254 24
[FW-Ethernet2/0/0]quit
[FW]interface vlanif 1
[FW-Vlanif1]undo ip address
```

在交换机上将G0/0/1与G0/0/21接口定义到VLAN11。将G0/0/2、G0/0/3与G0/0/22接口定义到VLAN12。将G0/0/4与G0/0/23接口定义到VLAN13。

```
[Quidway]sysname S1
[S1]vlan batch 11 to 13
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 11
[S1-GigabitEthernet0/0/1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 12
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 12
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/4
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 13
[S1-GigabitEthernet0/0/3]interface GigabitEthernet 0/0/21
```

```
[S1-GigabitEthernet0/0/21]port link-type access
[S1-GigabitEthernet0/0/21]port default vlan 11
[S1-GigabitEthernet0/0/21]interface GigabitEthernet 0/0/22
[S1-GigabitEthernet0/0/22]port link-type access
[S1-GigabitEthernet0/0/22]port default vlan 12
[S1-GigabitEthernet0/0/22]interface GigabitEthernet 0/0/23
[S1-GigabitEthernet0/0/23]port link-type access
[S1-GigabitEthernet0/0/23]port default vlan 13
```

步骤二. 配置静态路由，实现网络的连通性

在R2、R3和R4上配置缺省路由，在FW上配置明确的静态路由，实现四个Loopback0接口连接的网段之间的互通。R1无需定义缺省路由，原因是其作为Internet设备，它不需要知道内部和DMZ区域的私有网络信息。

```
[R2]ip route-static 0.0.0.0 0 10.0.20.254

[R3]ip route-static 0.0.0.0 0 10.0.20.254

[R4]ip route-static 0.0.0.0 0 10.0.40.254

[FW]ip route-static 10.0.2.0 24 10.0.20.2
[FW]ip route-static 10.0.3.0 24 10.0.20.3
[FW]ip route-static 10.0.4.0 24 10.0.40.4
[FW]ip route-static 0.0.0.0 0 1.1.1.1
```

步骤三. 将接口配置到安全区域

防火墙上默认有四个区域，分别是“local “、” trust “、” untrust “、” dmz “。

实验中我们使用到“trust “、” untrust “和” dmz “三个区域。

```
[FW]firewall zone dmz
[FW-zone-dmz]add interface Ethernet 2/0/0
[FW-zone-dmz]firewall zone trust
[FW-zone-trust]add interface Vlanif 12
[FW-zone-trust]firewall zone untrust
[FW-zone-untrust]add interface Ethernet 0/0/0
```




步骤四. 配置区域间的安全过滤

配置从Trust区域的网段10.0.2.0和10.0.3.0发往Untrust区域的数据包被放行。从Untrust区域发往DMZ目标服务器10.0.4.4的Telnet和FTP请求被放行。

```
[FW]firewall session link-state check
[FW]policy interzone trust untrust outbound
[FW-policy-interzone-trust-untrust-outbound]policy 0
[FW-policy-interzone-trust-untrust-outbound-0]policy source 10.0.2.0 0.0.0.255
[FW-policy-interzone-trust-untrust-outbound-0]policy source 10.0.3.0 0.0.0.255
[FW-policy-interzone-trust-untrust-outbound-0]action permit
[FW-policy-interzone-trust-untrust-outbound-0]quit
[FW-policy-interzone-trust-untrust-outbound]quit
[FW]policy interzone dmz untrust inbound
[FW-policy-interzone-dmz-untrust-inbound]policy 0
[FW-policy-interzone-dmz-untrust-inbound-0]policy destination 10.0.4.4 0
[FW-policy-interzone-dmz-untrust-inbound-0]policy service service-set telnet
[FW-policy-interzone-dmz-untrust-inbound-0]policy service service-set ftp
[FW-policy-interzone-dmz-untrust-inbound-0]action permit
[FW-policy-interzone-dmz-untrust-inbound-0]quit
```

步骤五. 配置 Easy-IP，实现 Trust 区域到 Untrust 区域的访问

配置使用Easy-IP，进行NAT源地址转换。并且将NAT与接口进行绑定。

```
[FW]nat-policy interzone trust untrust outbound
[FW-nat-policy-interzone-trust-untrust-outbound]policy 0
[FW-nat-policy-interzone-trust-untrust-outbound-0]policy source 10.0.2.0
0.0.0.255
[FW-nat-policy-interzone-trust-untrust-outbound-0]action source-nat
[FW-nat-policy-interzone-trust-untrust-outbound-0]easy-ip Ethernet 0/0/0
```

配置完成后，验证Trust区域与Untrust区域之间的访问是否正常。

```
[R2]ping 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
```

```
  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss

[R2]ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=4 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/4 ms
```

注意，直接测试R2与10.0.1.1之间的连通性，显示不通。使用扩展Ping，指定了发送数据包的源地址为10.0.2.2后，实现了连通性。

原因是，直接发送数据包到10.0.1.1时，数据包的源地址为10.0.20.2，该地址不属于NAT转换的客户端地址范围。

```
[FW]display nat-policy interzone trust untrust outbound
10:46:37  2011/12/26
nat-policy interzone trust untrust outbound
 policy 0 (1 times matched)
  action source-nat
  policy service service-set ip
  policy source 10.0.2.0 0.0.0.255
  policy destination any
  easy-ip Ethernet0/0/0
```

步骤六.　配置 Address-Group，实现 Trust 区域到 Untrust 区域的访问

配置使用Address-Group，进行NAT源地址转换。并且将NAT与Address-Group进行绑定。

```
[FW]nat address-group 1 1.1.1.3 1.1.1.10
[FW]nat-policy interzone trust untrust outbound
```

```
[FW-nat-policy-interzone-trust-untrust-outbound]policy 1
[FW-nat-policy-interzone-trust-untrust-outbound-0]policy source 10.0.3.0
0.0.0.255
[FW-nat-policy-interzone-trust-untrust-outbound-0]action source-nat
[FW-nat-policy-interzone-trust-untrust-outbound-0]address-group 1
```

配置完成后，验证Trust区域与Untrust区域之间的访问是否正常。

```
[R3]ping -a 10.0.3.3 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=12 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=4 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/4/12 ms
```

使用扩展Ping，指定了发送数据包的源地址为10.0.3.3后，实现了连通性。

```
[FW]display nat-policy interzone trust untrust outbound
10:52:37  2011/12/26
nat-policy interzone trust untrust outbound
 policy 0 (1 times matched)
  action source-nat
  policy service service-set ip
  policy source 10.0.2.0 0.0.0.255
  policy destination any
  easy-ip Ethernet0/0/0

 policy 1 (1 times matched)
  action source-nat
  policy service service-set ip
  policy source 10.0.3.0 0.0.0.255
  policy destination any
  address-group 1
```

Trust区域的10.0.2.0/24和10.0.3.0/24都可以实现到Untrust区域的访问。

步骤七. 将内网服务器 10.0.4.4 发布出去

配置内网服务器10.0.4.4的Telnet和FTP服务，映射到地址1.1.1.100。

```
[FW]nat server protocol tcp global 1.1.1.100 telnet inside 10.0.4.4 telnet
[FW]nat server protocol tcp global 1.1.1.100 ftp inside 10.0.4.4 ftp
```

FTP是多通道协议，NAT转换过程中需要配置NAT ALG功能。

在DMZ和Untrust域间配置NAT ALG，使服务器可以正常对外提供FTP服务。

```
[FW]firewall interzone dmz untrust
[FW-interzone-dmz-untrust]detect ftp
```

在R4上开启Telnet和FTP功能，并在R1上测试，测试时需注意，对外发布的地址为1.1.1.100，所以R1对10.0.4.4访问时，访问的目标地址应为1.1.1.100。

```
[R4]aaa
[R4-aaa]local-user huawei password simple huawei
[R4-aaa]local-user huawei service-type ftp
[R4-aaa]local-user huawei ftp-directory flash:
[R4-aaa]quit
[R4]user-interface vty 0 4
[R4-ui-vty0-4]authentication-mode none
[R4-ui-vty0-4]quit
[R4]ftp server enable

<R1>telnet 1.1.1.100
  Press CTRL_] to quit telnet mode
  Trying 1.1.1.100 ...
  Connected to 1.1.1.100 ...
<R4>quit
<R1>ftp 1.1.1.100
Trying 1.1.1.100 ...
Press CTRL+K to abort
Connected to 1.1.1.100.
220 FTP service ready.
User(1.1.1.100:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[R1-ftp]
```

Untrust区域可以访问DMZ区域1.1.1.100/24提供的Telnet和FTP服务。

步骤八. 配置域内 NAT，实现 Trust 区域能够访问 1.1.1.200

配置内网服务器10.0.3.3的NAT Server服务，映射到地址1.1.1.200。

```
[FW]nat server protocol tcp global 1.1.1.200 telnet inside 10.0.3.3 telnet
```

配置域内NAT， 内网用户访问1.1.1.200的源地址进行转换，转换为公网地址。

```
[FW]nat-policy zone trust
[FW-nat-policy-zone-trust]policy 0
[FW-nat-policy-zone-trust-0]policy source 10.0.2.0 0.0.0.255
[FW-nat-policy-zone-trust-0]policy destination 1.1.1.200 0
[FW-nat-policy-zone-trust-0]action source-nat
[FW-nat-policy-zone-trust-0]address-group 1
```

在R3上开启Telnet功能，并在R2上测试。测试时需注意，对外发布的地址为1.1.1.200，所以R2对10.0.3.3访问时，访问的目标地址应为1.1.1.200。

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode none

<R2>telnet -a 10.0.2.2 1.1.1.200
  Press CTRL_] to quit telnet mode
  Trying 1.1.1.200 ...
  Connected to 1.1.1.200 ...
<R3>
```

附加实验：思考并验证

思考一下，如果一个企业的防火墙同时接入两个运营商网络，该如何发布内部服务器提供的服务？

最终设备配置

```
[FW]display current-configuration
#
 sysname FW
#
 nat address-group 1 1.1.1.3 1.1.1.10
 nat server 0 protocol tcp global 1.1.1.100 telnet inside 10.0.4.4 telnet
 nat server 1 protocol tcp global 1.1.1.100 ftp inside 10.0.4.4 ftp
```

```
 nat server 2 protocol tcp global 1.1.1.200 telnet inside 10.0.3.3 telnet
#
vlan batch 1 12
#
 firewall session link-state check
#
interface Vlanif12
 ip address 10.0.20.254 255.255.255.0
#
interface Ethernet0/0/0
 ip address 1.1.1.254 255.255.255.0
#
interface Ethernet1/0/0
 portswitch
 port link-type access
 port access vlan 12
#
interface Ethernet2/0/0
 ip address 10.0.40.254 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface Vlanif12
#
firewall zone untrust
 set priority 5
 add interface Ethernet0/0/0
#
firewall zone dmz
 set priority 50
 add interface Ethernet2/0/0
#
firewall interzone dmz untrust
 detect ftp
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
 ip route-static 10.0.2.0 255.255.255.0 10.0.20.2
 ip route-static 10.0.3.0 255.255.255.0 10.0.20.3
 ip route-static 10.0.4.0 255.255.255.0 10.0.40.4
#
policy interzone trust untrust outbound
 policy 0
  action permit
```

```
  policy source 10.0.2.0 0.0.0.255
  policy source 10.0.3.0 0.0.0.255
#
policy interzone dmz untrust inbound
 policy 0
  action permit
  policy service service-set ftp
  policy service service-set telnet
  policy destination 10.0.4.4 0
#
nat-policy interzone trust untrust outbound
 policy 0
  action source-nat
  policy source 10.0.2.0 0.0.0.255
  easy-ip Ethernet0/0/0

 policy 1
  action source-nat
  policy source 10.0.3.0 0.0.0.255
  address-group 1
#
nat-policy zone trust
 policy 0
  action source-nat
  policy source 10.0.2.0 0.0.0.255
  policy destination 1.1.1.200 0
  address-group 1
#
Return

<R1>display current-configuration
[V200R001C00SPC200]
#
 sysname R1
#
#
interface GigabitEthernet0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
Return
```

```
<R2>display current-configuration
[V200R001C00SPC200]
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.2 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
#
Return
```

```
[R3]display current-configuration
[V200R001C00SPC200]
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
#
user-interface vty 0 4
 authentication-mode none
#
Return
```

```
[R4]display current-configuration
[V200R001C00SPC500]
#
 sysname R4
 ftp server enable
#
#
aaa
 local-user huawei password simple huawei
```

```
 local-user huawei ftp-directory flash:
 local-user huawei service-type ftp
#
interface GigabitEthernet0/0/1
 ip address 10.0.40.4 255.255.255.0
#
interface LoopBack0
 ip address 10.0.4.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.40.254
#
user-interface vty 0 4
 authentication-mode none
#
Return

<S1>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S1
#
 vlan batch 11 to 13
#
 interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 13
#
interface GigabitEthernet0/0/21
 port link-type access
 port default vlan 11
#
```

```
interface GigabitEthernet0/0/22
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/23
 port link-type access
 port default vlan 13
#
Return
```

实验 1-5 USG 防火墙双机热备份

学习目的

- 掌握防火墙双机热备份概念
- 掌握对防火墙的VRRP配制方法
- 掌握防火墙HRP的配制方法

拓扑图

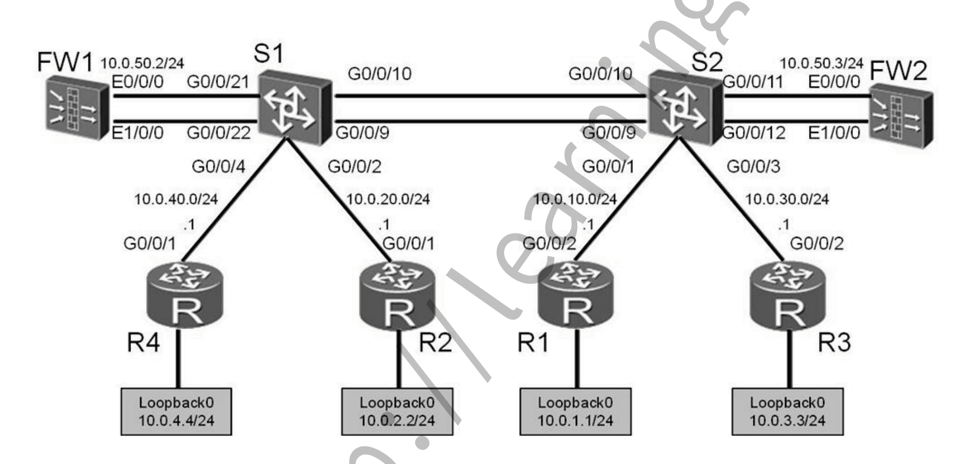


图1-5-1 USG防火墙区域配置物理拓扑图

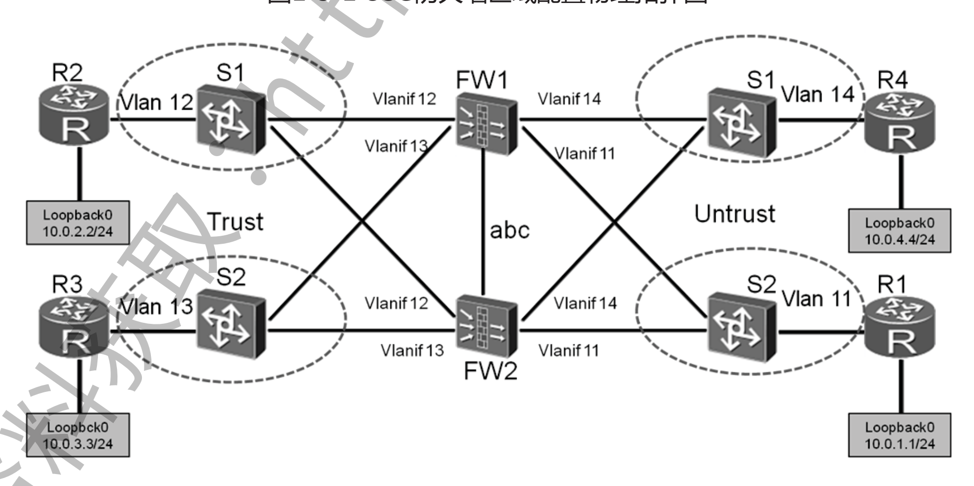


图1-5-2 USG防火墙区域配置逻辑拓扑图

场景

你是你们公司的网络管理员，现在公司为了保证通讯可靠性，需要配置防火墙双机热备份。

你针对目前通讯需求，配置基于负载分担的防火墙双机热备份。正常情况下，Trust区域访问Untrust区域时，不同路由发出的数据包默认由各自的主用防火墙转发，实现负载分担；设备故障时，数据包流量切换到备用防火墙转发，实现热备份。

学习任务

步骤一. 基本配置与 IP 编址

给所有路由器配置IP地址和掩码。配置时注意所有的Loopback接口配置掩码均为24位。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.0.10.1 24
[R1-GigabitEthernet0/0/2]interface loopback 0
[R1-LoopBack0]ip address 10.0.1.1 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.20.1 24
[R2-GigabitEthernet0/0/1]interface loopback 0
[R2-LoopBack0]ip address 10.0.2.2 24

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/1]ip address 10.0.30.1 24
[R3-GigabitEthernet0/0/1]interface loopback 0
[R3-LoopBack0]ip address 10.0.3.3 24

<Huawei>system-view
```

```
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.40.1 24
[R4-GigabitEthernet0/0/1]interface loopback 0
[R4-LoopBack0]ip address 10.0.4.4 24
```

在两个防火墙上配置VLAN11、12、13和14，并配置相应的三层接口地址。给防火墙配置地址时，需要注意Ethernet1/0/0接口为二层交换机接口，无法配置IP地址。另外由于默认防火墙会给它的Vlanif1配置地址，实验中为避免干扰，删除该配置。

```
<FW1>system-view
[FW1]vlan batch 11 to 14
[FW1]interface vlanif 11
[FW1-Vlanif11]ip address 10.0.10.2 24
[FW1-Vlanif11]interface vlanif 12
[FW1-Vlanif12]ip address 10.0.20.2 24
[FW1-Vlanif12]interface Vlanif 13
[FW1-Vlanif13]ip address 10.0.30.2 24
[FW1-Vlanif13]interface Vlanif 14
[FW1-Vlanif14]ip address 10.0.40.2 24
[FW1-Vlanif14]interface Ethernet0/0/0
[FW1-Ethernet0/0/0]ip address 10.0.50.2 24
[FW1-Ethernet0/0/0]quit
[FW1]interface vlanif 1
[FW1-Vlanif1]undo ip address

<FW2>system-view
[FW2]vlan batch 11 to 14
[FW2]interface vlanif 11
[FW2-Vlanif11]ip address 10.0.10.3 24
[FW2-Vlanif11]interface vlanif 12
[FW2-Vlanif12]ip address 10.0.20.3 24
[FW2-Vlanif12]interface Vlanif 13
[FW2-Vlanif13]ip address 10.0.30.3 24
[FW2-Vlanif13]interface Vlanif 14
[FW2-Vlanif14]ip address 10.0.40.3 24
[FW2-Vlanif14]interface Ethernet0/0/0
[FW2-Ethernet0/0/0]ip address 10.0.50.3 24
[FW2-Ethernet0/0/0]quit
[FW2]interface vlanif 1
[FW2-Vlanif1]undo ip address
```

交换机上需要按照需求定义VLAN。

```
<S1>system-view
[S1]vlan batch 11 to 14
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 12
[S1-GigabitEthernet0/0/2]interface gigabitEthernet 0/0/4
[S1-GigabitEthernet0/0/4]port link-type access
[S1-GigabitEthernet0/0/4]port default vlan 14

<S2>system-view
[S2]vlan batch 11 to 14
[S2]interface GigabitEthernet 0/0/1
[S2-GigabitEthernet0/0/1]port link-type access
[S2-GigabitEthernet0/0/1]port default vlan 11
[S2-GigabitEthernet0/0/1]interface gigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]port link-type access
[S2-GigabitEthernet0/0/3]port default vlan 13
```

将S1的接口G0/0/9与S2的接口G0/0/9改为Trunk类型，允许VLAN11、12、13和14通过。

```
[S1]interface GigabitEthernet 0/0/9
[S1-GigabitEthernet0/0/9]port link-type trunk
[S1-GigabitEthernet0/0/9]port trunk allow-pass vlan 11 to 14
[S1-GigabitEthernet0/0/9]quit

[S2]interface GigabitEthernet 0/0/9
[S2-GigabitEthernet0/0/9]port link-type trunk
[S2-GigabitEthernet0/0/9]port trunk allow-pass vlan 11 to 14
[S2-GigabitEthernet0/0/9]quit
```

把S1的接口G0/0/21、G0/0/10和S2的接口G0/0/10、G0/0/11划到一个VLAN中，定义属于VLAN10。该链路为防火墙心跳线发送数据。

我们为VLAN10启用MSTP协议，防止MSTP协议的默认进程0关闭S1与S2的G0/0/10接口。

需要注意的是，两台交换机上配置的Region-name必须一致，我们设置Region-name为FW。

```
[S1]vlan 10
[S1-vlan10]quit
[S1]interface GigabitEthernet 0/0/21
[S1-GigabitEthernet0/0/21]port link-type access
```

```
[S1-GigabitEthernet0/0/21]port default vlan 10
[S1-GigabitEthernet0/0/21]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]port link-type access
[S1-GigabitEthernet0/0/10]port default vlan 10
[S1-GigabitEthernet0/0/10]quit
[S1]stp region-configuration
[S1-mst-region]region-name FW
[S1-mst-region]instance 1 vlan 10
[S1-mst-region]active region-configuration

[S2]vlan 10
[S2-vlan10]quit
[S2]interface GigabitEthernet 0/0/11
[S2-GigabitEthernet0/0/11]port link-type access
[S2-GigabitEthernet0/0/11]port default vlan 10
[S2-GigabitEthernet0/0/11]interface GigabitEthernet 0/0/10
[S2-GigabitEthernet0/0/10]port link-type access
[S2-GigabitEthernet0/0/10]port default vlan 10
[S2-GigabitEthernet0/0/10]quit
[S2]stp region-configuration
[S2-mst-region]region-name FW
[S2-mst-region]instance 1 vlan 10
[S2-mst-region]active region-configuration
```

将FW1的接口E1/0/0与S1的接口G0/0/22改为Trunk类型，允许通过VLAN11、12、13和14。将FW2的接口E1/0/0与S2的接口G0/0/12改为Trunk类型，允许通过VLAN11、12、13和14。

```
[FW1]interface Ethernet1/0/0
[FW1]port link-type trunk
[FW1]port trunk permit vlan 11 to 14

[S1]interface GigabitEthernet 0/0/22
[S1]port link-type trunk
[S1]port trunk allow-pass vlan 11 to 14

[FW2]interface Ethernet1/0/0
[FW2]port link-type trunk
[FW2]port trunk permit vlan 11 to 14

[S2]interface GigabitEthernet 0/0/12
[S2]port link-type trunk
[S2]port trunk allow-pass vlan 11 to 14
```

步骤二. 将接口划分到安全区域

防火墙上默认有四个区域，分别是“Local “、” Trust “、” Untrust “、” DMZ “。

实验中我们使用到默认的“Trust “和” Untrust “两个区域，将vlanif12、vlanif13划分到trust区域，将vlanif11、vlanif14划分到Untrust区域。在两个防火墙上分别自定义一个abc区域，设置优先级为80，将心跳线接口Ethernet0/0/0划分进该区域。

```
[FW1]firewall zone trust
[FW1-zone-trust]add interface vlanif 12
[FW1-zone-trust]add interface vlanif 13
[FW1-zone-trust]firewall zone untrust
[FW1-zone-untrust]add interface vlanif 11
[FW1-zone-untrust]add interface vlanif 14
[FW1-zone-untrust]firewall zone name abc
[FW1-zone-abc]set priority 80
[FW1-zone-abc]add interface Ethernet 0/0/0
[FW1-zone-abc]quit
[FW1]firewall packet-filter default permit all

[FW2]firewall zone trust
[FW2-zone-trust]add interface vlanif 12
[FW2-zone-trust]add interface vlanif 13
[FW2-zone-trust]firewall zone untrust
[FW2-zone-untrust]add interface vlanif 11
[FW2-zone-untrust]add interface vlanif 14
[FW2-zone-untrust]firewall zone name abc
[FW2-zone-abc]set priority 80
[FW2-zone-abc]add interface Ethernet 0/0/0
[FW2-zone-abc]quit
[FW2]firewall packet-filter default permit all
```

完成配置后测试连通性。

```
[FW1]ping 10.0.20.1
09:47:13  2011/12/27
  PING 10.0.20.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.20.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=5 ttl=255 time=1 ms
```

```
  --- 10.0.20.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[FW1]ping 10.0.30.1
09:47:35  2011/12/27
  PING 10.0.30.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.30.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.30.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[FW1]ping 10.0.40.1
09:48:01  2011/12/27
  PING 10.0.40.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.40.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.40.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.40.1: bytes=56 Sequence=3 ttl=255 time=190 ms
    Reply from 10.0.40.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.40.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.40.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/38/190 ms

[FW1]ping 10.0.10.1
09:48:34  2011/12/27
  PING 10.0.10.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=3 ttl=255 time=1 ms
```

```
    Reply from 10.0.10.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.10.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[FW2]ping 10.0.10.1
03:51:04  2011/12/27
  PING 10.0.10.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.10.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.10.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.10.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[FW2]ping 10.0.20.1
03:51:23  2011/12/27
  PING 10.0.20.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.20.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.20.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.20.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[FW2]ping 10.0.30.1
03:51:47  2011/12/27
  PING 10.0.30.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.30.1: bytes=56 Sequence=1 ttl=255 time=1 ms
```

```
    Reply from 10.0.30.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.30.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.0.30.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

[FW2]ping 10.0.40.1
03:52:15  2011/12/27
  PING 10.0.40.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.40.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.0.40.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.0.40.1: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 10.0.40.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.0.40.1: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 10.0.40.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/4/10 ms
```

步骤三. 配置防火墙 VRRP 备份组

在FW1上配置各VRRP备份组，并配置备份组的虚拟IP地址。

```
[FW1]interface vlanif 12
[FW1-Vlanif12]vrrp vrid 12 virtual-ip 10.0.20.254 master
[FW1-Vlanif12]interface vlanif 13
[FW1-Vlanif13]vrrp vrid 13 virtual-ip 10.0.30.254 slave
[FW1-Vlanif13]interface vlanif 14
[FW1-Vlanif14]vrrp vrid 14 virtual-ip 10.0.40.254 master
[FW1-Vlanif14]interface vlanif 11
[FW1-Vlanif11]vrrp vrid 11 virtual-ip 10.0.10.254 slave
```

在FW2上配置各VRRP备份组，并配置备份组的虚拟IP地址。

FW2和上述FW1的配置基本相同，不同之处在于FW2上配置VRRP备份组时，

与FW1的Master管理组对应的必须配置为Slave管理组，与FW1的Slave管理组对应的必须配置为Master管理组。

```
[FW2]interface vlanif 12
[FW2-Vlanif12]vrrp vrid 12 virtual-ip 10.0.20.254 slave
[FW2-Vlanif12]interface vlanif 13
[FW2-Vlanif13]vrrp vrid 13 virtual-ip 10.0.30.254 master
[FW2-Vlanif13]interface vlanif 14
[FW2-Vlanif14]vrrp vrid 14 virtual-ip 10.0.40.254 slave
[FW2-Vlanif14]interface vlanif 11
[FW2-Vlanif11]vrrp vrid 11 virtual-ip 10.0.10.254 master
```

查看备份组配置情况，检查VRRP Group状态是否与命令一致。

```
[FW1]display vrrp
20:56:41  2011/12/28
  Vlanif13 | Virtual Router 13
    VRRP Group : Slave
    state : Backup
    Virtual IP : 10.0.30.254
    Virtual MAC : 0000-5e00-010d
    Primary IP : 10.0.30.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  Vlanif11 | Virtual Router 11
    VRRP Group : Slave
    state : Backup
    Virtual IP : 10.0.10.254
    Virtual MAC : 0000-5e00-010b
    Primary IP : 10.0.10.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

```
  Vlanif14 | Virtual Router 14
    VRRP Group : Master
    state : Backup
    Virtual IP : 10.0.40.254
    Virtual MAC : 0000-5e00-010e
    Primary IP : 10.0.40.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  Vlanif12 | Virtual Router 12
    VRRP Group : Master
    state : Backup
    Virtual IP : 10.0.20.254
    Virtual MAC : 0000-5e00-010c
    Primary IP : 10.0.20.2
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

[FW2]display vrrp
14:32:32  2011/12/28
  Vlanif11 | Virtual Router 11
    VRRP Group : Master
    state : Master
    Virtual IP : 10.0.10.254
    Virtual MAC : 0000-5e00-010b
    Primary IP : 10.0.10.3
    PriorityRun : 100
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

```
Vlanif14 | Virtual Router 14
  VRRP Group : Slave
  state : Master
  Virtual IP : 10.0.40.254
  Virtual MAC : 0000-5e00-010e
  Primary IP : 10.0.40.3
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES

Vlanif13 | Virtual Router 13
  VRRP Group : Master
  state : Master
  Virtual IP : 10.0.30.254
  Virtual MAC : 0000-5e00-010d
  Primary IP : 10.0.30.3
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES

Vlanif12 | Virtual Router 12
  VRRP Group : Slave
  state : Master
  Virtual IP : 10.0.20.254
  Virtual MAC : 0000-5e00-010c
  Primary IP : 10.0.20.3
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES
```

步骤四. 配置 HRP 备份通道

分别在FW1和FW2上配置备份通道接口，并启用HRP。注意，防火墙工作于双机热备份组网环境下，如果报文的来回路径不一致，可以利用命令**hrp mirror session enable**配置会话快速备份功能，保证主用防火墙的会话信息立即同步至备用防火墙。

当主用防火墙出现故障时，后续报文能够被备用防火墙转发出去，从而保证内外部用户的会话不中断。

```
[FW1]hrp interface Ethernet0/0/0
[FW1]hrp mirror session enable
[FW1]hrp enable

[FW2]hrp interface Ethernet0/0/0
[FW2]hrp mirror session enable
[FW2]hrp enable
```

注意在此步骤后，设备配置的提示符名称会根据设备的HRP状态，增加**HRP_M或HRP_S**。

成功配置备份通道之后，主备防火墙之间根据配置协商**master/backup**状态，检查此刻防火墙VRRP状态。

```
HRP_M[FW1]display vrrp
21:32:17  2011/12/28
  Vlanif13 | Virtual Router 13
    VRRP Group : Slave
    state : Backup
    Virtual IP : 10.0.30.254
    Virtual MAC : 0000-5e00-010d
    Primary IP : 10.0.30.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  Vlanif11 | Virtual Router 11
    VRRP Group : Slave
    state : Backup
    Virtual IP : 10.0.10.254
```

```
    Virtual MAC : 0000-5e00-010b
    Primary IP : 10.0.10.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  Vlanif14 | Virtual Router 14
    VRRP Group : Master
    state : Master
    Virtual IP : 10.0.40.254
    Virtual MAC : 0000-5e00-010e
    Primary IP : 10.0.40.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  Vlanif12 | Virtual Router 12
    VRRP Group : Master
    state : Master
    Virtual IP : 10.0.20.254
    Virtual MAC : 0000-5e00-010c
    Primary IP : 10.0.20.2
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

HRP_S[FW2]display vrrp
15:08:31  2011/12/28
  Vlanif11 | Virtual Router 11
    VRRP Group : Master
    state : Master
```

```
  Virtual IP : 10.0.10.254
  Virtual MAC : 0000-5e00-010b
  Primary IP : 10.0.10.3
  PriorityRun : 120
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES

Vlanif14 | Virtual Router 14
  VRRP Group : Slave
  state : Backup
  Virtual IP : 10.0.40.254
  Virtual MAC : 0000-5e00-010e
  Primary IP : 10.0.40.3
  PriorityRun : 120
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES

Vlanif13 | Virtual Router 13
  VRRP Group : Master
  state : Master
  Virtual IP : 10.0.30.254
  Virtual MAC : 0000-5e00-010d
  Primary IP : 10.0.30.3
  PriorityRun : 120
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES

Vlanif12 | Virtual Router 12
  VRRP Group : Slave
  state : Backup
  Virtual IP : 10.0.20.254
```



```
Virtual MAC : 0000-5e00-010c
Primary IP : 10.0.20.3
PriorityRun : 120
PriorityConfig : 100
MasterPriority : 120
Preempt : YES   Delay Time : 0
Advertisement Timer : 1
Auth Type : NONE
Check TTL : YES
```

步骤五. 配置区域间包过滤策略

当FW1和FW2都启动HRP功能完成后，在FW1上开启配置命令的自动备份，这样在FW1上配置的域间包过滤规则都将自动备份到FW2。

```
HRP_M[FW1]hrp auto-sync config
```

默认配置下安全区域之间是互通的，现配置区域间包过滤策略，关闭各区域间的互通。仅允许Trust区域访问Untrust区域，不允许其他区域之间的访问。

```
HRP_M[FW1]firewall packet-filter default deny all
HRP_M[FW1]firewall packet-filter default permit interzone trust untrust direction outbound
```

步骤六. HRP_M[FW1]firewall session link-state check 配置静态路由，实现网络连通性

在R1、R2、R3和R4上配置默认网关，在FW1与FW2上配置明确的静态路由，实现网络的连通性。

```
[R1]ip route-static 0.0.0.0 0 10.0.10.254

[R2]ip route-static 0.0.0.0 0 10.0.20.254

[R3]ip route-static 0.0.0.0 0 10.0.30.254

[R4]ip route-static 0.0.0.0 0 10.0.40.254

HRP_M[FW1]ip route-static 10.0.1.0 24 10.0.10.1
HRP_M[FW1]ip route-static 10.0.2.0 24 10.0.20.1
HRP_M[FW1]ip route-static 10.0.3.0 24 10.0.30.1
```

```
HRP_M[FW1]ip route-static 10.0.4.0 24 10.0.40.1

HRP_S[FW2]ip route-static 10.0.1.0 24 10.0.10.1
HRP_S[FW2]ip route-static 10.0.2.0 24 10.0.20.1
HRP_S[FW2]ip route-static 10.0.3.0 24 10.0.30.1
HRP_S[FW2]ip route-static 10.0.4.0 24 10.0.40.1
```

配置完成后，测试Trust区域与Untrust区域通讯状况。

```
[R2]ping -a 10.0.2.2 10.0.1.1
  PING 10.0.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.1: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=2 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.1.1: bytes=56 Sequence=4 ttl=254 time=5 ms
    Reply from 10.0.1.1: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/5 ms

[R2]ping -a 10.0.2.2 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.4: bytes=56 Sequence=1 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=2 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=3 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=4 ttl=254 time=5 ms
    Reply from 10.0.4.4: bytes=56 Sequence=5 ttl=254 time=3 ms

  --- 10.0.4.4 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/4/5 ms

[R3]ping -a 10.0.3.3 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.4: bytes=56 Sequence=1 ttl=254 time=5 ms
    Reply from 10.0.4.4: bytes=56 Sequence=2 ttl=254 time=5 ms
    Reply from 10.0.4.4: bytes=56 Sequence=3 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=4 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=5 ttl=254 time=6 ms
```

```
--- 10.0.4.4 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/6 ms
```

步骤七. 双机热备份测试

R2与R4的数据包，默认是通过防火墙FW1转发，并且防火墙FW2作为备份。

设置场景，在R2于R4通讯过程中，FW1上Vlanif12接口发生故障。通讯依然正常。

我们从R2上发送20个数据包给R4。在发送过程中将防火墙上的Vlanif 12接口关闭以模拟接口故障，并查看通讯状态。

注意，在执行**ping**命令过程中，须尽快将FW1上Vlanif12接口关闭，要在数据包发送结束之前关闭该接口。

```
[R2]ping -c 20 -a 10.0.2.2 10.0.4.4

HRP_S[FW1]interface vlanif 12
HRP_S[FW1-Vlanif12]shutdown
```

我们可以看见，通讯依然正常，即使FW1上的Vlanif12接口故障，仍然没有数据包的丢失。

```
[R2]ping -c 20 -a 10.0.2.2 10.0.4.4
  PING 10.0.4.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.4.4: bytes=56 Sequence=1 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=2 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=3 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=4 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=5 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=6 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=7 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=8 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=9 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=10 ttl=254 time=5 ms
    Reply from 10.0.4.4: bytes=56 Sequence=11 ttl=254 time=3 ms
    Reply from 10.0.4.4: bytes=56 Sequence=12 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=13 ttl=254 time=4 ms
    Reply from 10.0.4.4: bytes=56 Sequence=14 ttl=254 time=3 ms
```

```
  Reply from 10.0.4.4: bytes=56 Sequence=15 ttl=254 time=4 ms
  Reply from 10.0.4.4: bytes=56 Sequence=16 ttl=254 time=4 ms
  Reply from 10.0.4.4: bytes=56 Sequence=17 ttl=254 time=3 ms
  Reply from 10.0.4.4: bytes=56 Sequence=18 ttl=254 time=4 ms
  Reply from 10.0.4.4: bytes=56 Sequence=19 ttl=254 time=3 ms
  Reply from 10.0.4.4: bytes=56 Sequence=20 ttl=254 time=3 ms

 --- 10.0.4.4 ping statistics ---
  20 packet(s) transmitted
  20 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/3/5 ms
```

此时查看防火墙FW2的VRRP状态，发现FW2上接口Vlanif12与Vlanif14已经同时转换为Master状态。即FW1上接口Vlanif12出现故障时，FW2上的备份接口立即从Backup状态转换成Master状态，引导数据包转发。

```
HRP_M[FW2]display vrrp
03:14:23  2011/12/29
 Vlanif11 | Virtual Router 11
  VRRP Group : Master
  state : Master
  Virtual IP : 10.0.10.254
  Virtual MAC : 0000-5e00-010b
  Primary IP : 10.0.10.3
  PriorityRun : 120
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES

 Vlanif14 | Virtual Router 14
  VRRP Group : Slave
  state : Master
  Virtual IP : 10.0.40.254
  Virtual MAC : 0000-5e00-010e
  Primary IP : 10.0.40.3
  PriorityRun : 120
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0
  Advertisement Timer : 1
```

```
    Auth Type : NONE
    Check TTL : YES

  Vlanif13 | Virtual Router 13
    VRRP Group : Master
    state : Master
    Virtual IP : 10.0.30.254
    Virtual MAC : 0000-5e00-010d
    Primary IP : 10.0.30.3
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES

  Vlanif12 | Virtual Router 12
    VRRP Group : Slave
    state : Master
    Virtual IP : 10.0.20.254
    Virtual MAC : 0000-5e00-010c
    Primary IP : 10.0.20.3
    PriorityRun : 120
    PriorityConfig : 100
    MasterPriority : 120
    Preempt : YES   Delay Time : 0
    Advertisement Timer : 1
    Auth Type : NONE
    Check TTL : YES
```

附加实验：思考并验证

当心跳线出现故障时，防火墙FW1与FW2的状态会是怎样的？Trust与Untrust区域之间通讯的数据包是如何转发的？

最终设备配置

```
<R1>display current-configuration
[V200R001C00SPC200]
#
```

```
 sysname R1
#
interface GigabitEthernet0/0/2
 ip address 10.0.10.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.10.254
#
return

<R2>display current-configuration
[V200R001C00SPC200]
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 10.0.20.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.2.2 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.20.254
#
return

<R3>display current-configuration
[V200R001C00SPC200]
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.0.30.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.3.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.30.254
#
return

<R4>display current-configuration
```

```
[V200R001C00SPC500]
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 10.0.40.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.4.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.40.254
#
return

<S1>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S1
#
 vlan batch 10 to 14
#
 stp region-configuration
  region-name FW
  instance 1 vlan 10
  active region-configuration
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 12
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 14
#
interface GigabitEthernet0/0/9
 port link-type trunk
 port trunk allow-pass vlan 11 to 14
#
interface GigabitEthernet0/0/10
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/21
```

```
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/22
 port link-type trunk
 port trunk allow-pass vlan 11 to 14
#
return

<S2>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S2
#
 vlan batch 10 to 14
#
 stp region-configuration
  region-name FW
  instance 1 vlan 10
  active region-configuration
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 13
#
interface GigabitEthernet0/0/9
 port link-type trunk
 port trunk allow-pass vlan 11 to 14
#
interface GigabitEthernet0/0/10
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/11
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/12
 port link-type trunk
```

```
 port trunk allow-pass vlan 11 to 14
#
return

HRP_M<FW1>display current-configuration
#
 sysname FW1
#
 hrp mirror session enable
 hrp enable
 hrp interface Ethernet0/0/0
#
 firewall packet-filter default deny interzone local trust direction inbound
 firewall packet-filter default deny interzone local trust direction outbound
 firewall packet-filter default deny interzone local untrust direction inbound
 firewall packet-filter default deny interzone local untrust direction outbound
 firewall packet-filter default deny interzone local dmz direction inbound
 firewall packet-filter default deny interzone local dmz direction outbound
 firewall packet-filter default deny interzone local abc direction inbound
 firewall packet-filter default deny interzone local abc direction outbound
 firewall packet-filter default deny interzone trust untrust direction inbound
 firewall packet-filter default deny interzone trust dmz direction inbound
 firewall packet-filter default deny interzone trust dmz direction outbound
 firewall packet-filter default deny interzone trust abc direction inbound
 firewall packet-filter default deny interzone trust abc direction outbound
 firewall packet-filter default deny interzone dmz untrust direction inbound
 firewall packet-filter default deny interzone dmz untrust direction outbound
 firewall packet-filter default deny interzone abc untrust direction inbound
 firewall packet-filter default deny interzone abc untrust direction outbound
 firewall packet-filter default deny interzone abc dmz direction inbound
 firewall packet-filter default deny interzone abc dmz direction outbound
#
 undo firewall ipv6 session link-state check
#
 vlan batch 1 11 to 14
#
 undo firewall session link-state check
#
#
 runmode firewall
#
interface Vlanif11
 ip address 10.0.10.2 255.255.255.0
```

```
 vrrp vrid 11 virtual-ip 10.0.10.254 slave
#
interface Vlanif12
 ip address 10.0.20.2 255.255.255.0
 vrrp vrid 12 virtual-ip 10.0.20.254 master
#
interface Vlanif13
 ip address 10.0.30.2 255.255.255.0
 vrrp vrid 13 virtual-ip 10.0.30.254 slave
#
interface Vlanif14
 ip address 10.0.40.2 255.255.255.0
 vrrp vrid 14 virtual-ip 10.0.40.254 master
#
interface Ethernet0/0/0
 ip address 10.0.50.2 255.255.255.0
#
interface Ethernet1/0/0
 portswitch
 port link-type trunk
 port trunk permit vlan 1 11 to 14
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Vlanif12
 add interface Vlanif13
#
firewall zone untrust
 set priority 5
 add interface Vlanif11
 add interface Vlanif14
#
firewall zone dmz
 set priority 50
#
firewall zone name abc
 set priority 80
 add interface Ethernet0/0/0
#
nqa-jitter tag-version 1
```

```
#
 ip route-static 10.0.1.0 255.255.255.0 10.0.10.1
 ip route-static 10.0.2.0 255.255.255.0 10.0.20.1
 ip route-static 10.0.3.0 255.255.255.0 10.0.30.1
 ip route-static 10.0.4.0 255.255.255.0 10.0.40.1
#
 slb
#
cwmp
#
right-manager server-group
#
return

HRP_S<FW2>display current-configuration
#
 sysname FW2
#
 hrp mirror session enable
 hrp enable
 hrp interface Ethernet0/0/0
#
 firewall packet-filter default deny interzone local trust direction inbound
 firewall packet-filter default deny interzone local trust direction outbound
 firewall packet-filter default deny interzone local untrust direction inbound
 firewall packet-filter default deny interzone local untrust direction outbound
 firewall packet-filter default deny interzone local dmz direction inbound
 firewall packet-filter default deny interzone local dmz direction outbound
 firewall packet-filter default deny interzone local abc direction inbound
 firewall packet-filter default deny interzone local abc direction outbound
 firewall packet-filter default deny interzone trust untrust direction inbound
 firewall packet-filter default deny interzone trust dmz direction inbound
 firewall packet-filter default deny interzone trust dmz direction outbound
 firewall packet-filter default deny interzone trust abc direction inbound
 firewall packet-filter default deny interzone trust abc direction outbound
 firewall packet-filter default deny interzone dmz untrust direction inbound
 firewall packet-filter default deny interzone dmz untrust direction outbound
 firewall packet-filter default deny interzone abc untrust direction inbound
 firewall packet-filter default deny interzone abc untrust direction outbound
 firewall packet-filter default deny interzone abc dmz direction inbound
 firewall packet-filter default deny interzone abc dmz direction outbound
#
 undo firewall ipv6 session link-state check
```

```
#
 vlan batch 1 11 to 14
#
 undo firewall session link-state check
#
interface Vlanif11
 ip address 10.0.10.3 255.255.255.0
 vrrp vrid 11 virtual-ip 10.0.10.254 master
#
interface Vlanif12
 ip address 10.0.20.3 255.255.255.0
 vrrp vrid 12 virtual-ip 10.0.20.254 slave
#
interface Vlanif13
 ip address 10.0.30.3 255.255.255.0
 vrrp vrid 13 virtual-ip 10.0.30.254 master
#
interface Vlanif14
 ip address 10.0.40.3 255.255.255.0
 vrrp vrid 14 virtual-ip 10.0.40.254 slave
#
interface Ethernet0/0/0
 ip address 10.0.50.3 255.255.255.0
#
interface Ethernet1/0/0
 portswitch
 port link-type trunk
 port trunk permit vlan 1 11 to 14
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Vlanif12
 add interface Vlanif13
#
firewall zone untrust
 set priority 5
 add interface Vlanif11
 add interface Vlanif14
#
firewall zone dmz
```

```
 set priority 50
#
firewall zone name abc
 set priority 80
 add interface Ethernet0/0/0
#
nqa-jitter tag-version 1
#
 ip route-static 10.0.1.0 255.255.255.0 10.0.10.1
 ip route-static 10.0.2.0 255.255.255.0 10.0.20.1
 ip route-static 10.0.3.0 255.255.255.0 10.0.30.1
 ip route-static 10.0.4.0 255.255.255.0 10.0.40.1
#
slb
#
cwmp
#
right-manager server-group
#
return
```

第二章 服务质量与流量控制

实验 2-1 QoS 基础

学习目的

- 掌握使用NQA分析SLA的方法
- 掌握进行优先级映射和流量监管的方法
- 掌握配置流量整形的方法
- 掌握实现基于队列和基于流分类的拥塞管理方法
- 掌握配置WRED实现拥塞避免的方法

拓扑图

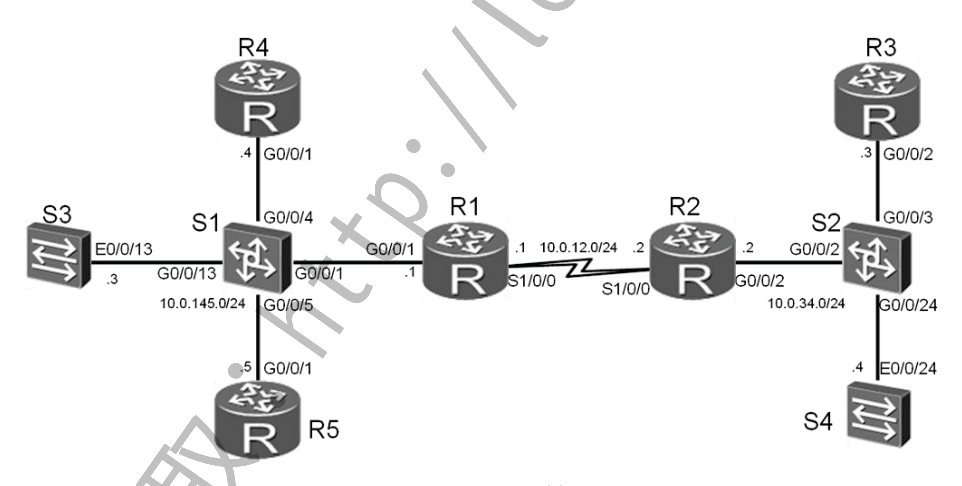


图2-1 QoS基础

场景

你是公司的网络管理员。公司网络分成两部分，其中R1与S1在公司总部，R2与S2在公司分部，之间通过专线实现互联。

随着网络的发展，内网带宽逐渐增大，而专线的带宽一直没有升级，所以网络中出现了比较严重的重要业务反应较慢，或无法正常使用的情况。

使用QoS的差分服务，你可以调整相应的QoS特性，保证重要的业务数据能更好的发送到目标。

实验中，S3和S4使用NQA相互发送数据，模拟大量数据流的发送。R3、R4与R5模拟客户端和服务器，测试重要应用是否可以正常使用。

学习任务

步骤一. 基础配置与 IP 编址

给所有路由器和交换机S3，S4配置IP地址和掩码。

配置时需要将R1接口S1/0/0的波特率配置为72000，作为广域网链路，因带宽不足而出现拥塞。

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R1
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 255.255.255.0
[R1-Serial1/0/0]baudrate 72000
[R1-Serial1/0/0]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.145.1 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R2
[R2]interface s1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 255.255.255.0
[R2-Serial1/0/0]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.34.2 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R3
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.34.3 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R4
```

```
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.145.4 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname R5
[R5]interface GigabitEthernet 0/0/1
[R5-GigabitEthernet0/0/1]ip address 10.0.145.5 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S3
[S3]interface vlan
[S3]interface Vlanif 1
[S3-Vlanif1]ip address 10.0.145.3 255.255.255.0

<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]sysname S4
[S4]interface Vlanif 1
[S4-Vlanif1]ip address 10.0.34.4 255.255.255.0
```

配置完成后，测试直连链路的连通性。

```
[R1]ping -c 1 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.12.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms

[R1]ping -c 1 10.0.145.3
  PING 10.0.145.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.3: bytes=56 Sequence=1 ttl=255 time=35 ms

  --- 10.0.145.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/35/35 ms
```

```
[R1]ping -c 1 10.0.145.4
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R1]ping -c 1 10.0.145.5
  PING 10.0.145.5: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.5: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.5 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R2]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=255 time=5 ms

  --- 10.0.34.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 5/5/5 ms

[R2]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms
```

步骤二. 配置静态路由与 NQA

在所有路由器和交换机S3，S4上配置静态路由。

```
[R1]ip route-static 10.0.34.0 255.255.255.0 10.0.12.2

[R2]ip route-static 10.0.145.0 255.255.255.0 10.0.12.1

[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2

[R4]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[R5]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S3]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S4]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
```

配置完成后，测试网络连通性。

```
[S3]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=252 time=40 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/40/40 ms

[R4]ping -c 1 10.0.34.3
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=3 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

[R5]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=253 time=44 ms
```

```
--- 10.0.34.3 ping statistics ---
  1 packet(s) transmitted
  1 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 44/44/44 ms
```

S3去往S4，R4，R5去往R3可以连通，证明网络通信正常。

公司总部和分部之间的链路为72K串行链路，因而在实际情况中很容易造成拥塞。

实验中使用NQA在网络中产生流量。S4作为NQA服务器端，S3作为NQA客户端。

定义UDP，Jitter两种NQA测试例，分别用来模拟企业网中的数据流量和语音流量。

通过设置NQA测试例中的一些参数来实现两种流量中任何一种单独存在的情况下不会产生拥塞，二者共存的情况下会产生拥塞，来模拟实际环境。

在S4设上配置NQA服务器端，UDP监听的IP地址设为10.0.34.4，端口号设为6000。

```
[S4]nqa-server udpecho 10.0.34.4 6000
```

在S3上配置UDP类型的NQA测试例模拟数据流量，其中**tos**设为28，包大小为5800字节，包间隔设为1s，周期设为3s，超时设为1s，并开启该测试。

```
[S3]nqa test-instance admin udp
[S3-nqa-admin-udp]test-type udp
[S3-nqa-admin-udp]destination-address ipv4 10.0.34.4
[S3-nqa-admin-udp]destination-port 6000
[S3-nqa-admin-udp]tos 28
[S3-nqa-admin-udp]datasize 5000
[S3-nqa-admin-udp]interval seconds 1
[S3-nqa-admin-udp]frequency 3
[S3-nqa-admin-udp]timeout 1
[S3-nqa-admin-udp]start now
```

查看UDP测试结果。

```
[S3]display nqa results test-instance admin udp
1 . Test 2 result   The test is finished
   Send operation times: 3                Receive response times: 3
   Completion:success                     RTD OverThresholds number: 0
   Attempts number:1                      Drop operation number:0
```

```
Disconnect operation number:0        Operation timeout number:0
System busy operation number:0       Connection fail number:0
Operation sequence errors number:0   RTT Stats errors number:0
Destination ip address:10.0.34.4
Min/Max/Average Completion Time: 930/950/943
Sum/Square-Sum  Completion Time: 2830/2669900
Last Good Probe Time: 2008-01-28 23:10:02.4
Lost packet ratio: 0 %
```

此时不丢包，链路没有产生拥塞。关闭UDP测试。

```
[S3]nqa test-instance admin udp
[S3-nqa-admin-udp]stop
```

在S3上配置Jitter类型的NQA测试例模拟语音流量，其中**tos**设为46，包大小为90字节，包间隔设为20ms，周期设为3s，超时设为1s，并开启该测试。

```
[S3]nqa test-instance admin jitter
[S3-nqa-admin-jitter]test-type jitter
[S3-nqa-admin-jitter]destination-address ipv4 10.0.34.4
[S3-nqa-admin-jitter]destination-port 6000
[S3-nqa-admin-jitter]tos 46
[S3-nqa-admin-jitter]datasize 90
[S3-nqa-admin-jitter]interval milliseconds 20
[S3-nqa-admin-jitter]frequency 3
[S3-nqa-admin-jitter]timeout 1
[S3-nqa-admin-jitter]start now
```

查看Jitter测试结果。

```
[S3]display nqa results test-instance admin jitter

 NQA entry(admin, jitter) :testflag is active ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:60
   Completion:success                    RTD OverThresholds number:0
   Min/Max/Avg/Sum RTT:40/70/54/3260     RTT  Square Sum:179800
   NumOfRTT:60                           Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:0
   Min Positive SD:10                    Min Positive DS:10
   Max Positive SD:10                    Max Positive DS:10
   Positive SD Number:5                  Positive DS Number:11
   Positive SD Sum:50                    Positive DS Sum:110
   Positive SD Square Sum:500            Positive DS Square Sum:1100
```

```
Min Negative SD:10                    Min Negative DS:10
Max Negative SD:10                    Max Negative DS:20
Negative SD Number:4                  Negative DS Number:10
Negative SD Sum:40                    Negative DS Sum:110
Negative SD Square Sum:400            Negative DS Square Sum:1300
Min Delay SD:20                       Min Delay DS:19
Avg Delay SD:27                       Avg Delay DS:26
Max Delay SD:35                       Max Delay DS:34
Packet Loss SD:0                      Packet Loss DS:0
Packet Loss Unknown:0                 jitter out value:0.0937500
jitter in value:0.2291667             NumberOfOWD:60
OWD SD Sum:1630                       OWD DS Sum:1570
TimeStamp unit: ms
```

此时不丢包，链路没有产生拥塞。关闭Jitter测试。

```
[S3]nqa test-instance admin jitter
[S3-nqa-admin-jitter]stop
```

步骤三. 配置优先级映射

现在通过**ping**命令来模拟公司中一些不太重要的流量，并且针对这部分流量，将其DSCP优先级映射为BE，不做QoS保证。

配置R1的接口G0/0/1与S1/0/0信任报文的DSCP优先级。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]trust dscp override
[R1-GigabitEthernet0/0/1]interface Serial 1/0/0
[R1-Serial1/0/0]trust dscp
```

在接口G0/0/1上的**trust**命令中需要加上**override**参数，使得接下来在R1上配置优先级映射后，将DSCP值修改为映射后的值。

在R4上使用**ping**命令产生去往R3的流量，并且将**tos**设为26。

```
[R4]ping -tos 26 10.0.34.3
```

在R1上配置优先级映射关系，将该流量的DSCP报文优先级26映射为0，

```
[R1]qos map-table dscp-dscp
[R1-maptbl-dscp-dscp]input 26 output 0
```

查看R1上的优先级映射信息。

```
[R1]display qos map-table dscp-dscp
Input DSCP      DSCP
-------------------
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
 8               8
 9               9
10              10
11              11
12              12
13              13
14              14
15              15
16              16
17              17
18              18
19              19
20              20
21              21
22              22
23              23
24              24
25              25
26               0
27              27
28              28
29              29
30              30
```

此时可以观察到，现在已将DSCP报文优先级26映射成为了0，而其余DSCP值都是默认映射值。

步骤四. 配置整形与监管

开启S3上的NQA的UDP与Jitter测试，模拟公司总部与分部之间的72K链路产生拥塞。

```
[S3]nqa test-instance admin udp
[S3-nqa-admin-udp]start now
[S3-nqa-admin-udp]nqa test-instance admin jitter
[S3-nqa-admin-jitter]start now
```

在R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=1944 ms
    Request time out

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    1 packet(s) received
    90.00% packet loss
    round-trip min/avg/max = 1944/1944/1944 ms
```

此时公司总部与分部之间的链路发生严重拥塞，丢包现象严重，即使通过的数据包延迟也非常大。此时R4无法与R3建立正常通信。

下面将介绍分别通过使用流量监管和流量整形的方法来消除链路上的拥塞，使得公司总部的客户端R4与分部的客户端R3能够建立正常通信。

首先通过流量监管来消除拥塞。在S1上，针对拥塞流量入接口G0/0/13上配置流量监管，CIR设为64kbit/s。

```
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]qos lr inbound cir 64
```

查看S1上流量监管的配置信息。

```
[S1]display qos lr inbound interface GigabitEthernet 0/0/13
GigabitEthernet0/0/13 lr inbound:
  cir: 64 Kbps, cbs: 8000 Byte
```

现在再回到R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=1412 ms
    Reply from 10.0.34.3: bytes=700 Sequence=2 ttl=253 time=255 ms
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=736 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=1746 ms
    Reply from 10.0.34.3: bytes=700 Sequence=5 ttl=253 time=246 ms
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=746 ms
    Reply from 10.0.34.3: bytes=700 Sequence=7 ttl=253 time=1736 ms
    Reply from 10.0.34.3: bytes=700 Sequence=8 ttl=253 time=258 ms
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=766 ms
    Reply from 10.0.34.3: bytes=700 Sequence=10 ttl=253 time=1736 ms

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 246/963/1746 ms
```

此时流量监管产生效果，不丢包，R4和R3之间能够建立起正常通信。

删除S1上流量监管配置。

```
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]undo qos lr inbound
```

现在通过流量整形的方式来达到消除拥塞的目的。在S3上，针对拥塞流量出接口E0/0/13上配置流量整形，CIR设为64kbit/s。

```
[S3]interface Ethernet0/0/13
[S3-Ethernet0/0/13]qos lr outbound cir 64
```

在R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=240 ms
    Reply from 10.0.34.3: bytes=700 Sequence=2 ttl=253 time=284 ms
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=334 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=224 ms
    Reply from 10.0.34.3: bytes=700 Sequence=5 ttl=253 time=344 ms
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=275 ms
```

```
    Reply from 10.0.34.3: bytes=700 Sequence=7 ttl=253 time=534 ms
    Reply from 10.0.34.3: bytes=700 Sequence=8 ttl=253 time=184 ms
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=204 ms
    Reply from 10.0.34.3: bytes=700 Sequence=10 ttl=253 time=314 ms

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 184/293/534 ms
```

此时流量监管产生效果，不丢包，R4和R3之间能够建立起正常通信。

删除S3上的流量整形配置，

```
[S3]interface Ethernet0/0/13
[S3-Ethernet0/0/13]undo qos lr outbound
```

现在再回到R4上使用**ping**命令实现模拟去往R3的流量，设置包大小为700字节，发10个包。

```
[R4]ping -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=1918 ms
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=1762 ms
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    2 packet(s) received
    80.00% packet loss
    round-trip min/avg/max = 1762/1840/1918 ms
```

删除配置之后，丢包严重，并且通过的数据包延迟也非常大。R4与R3之间无法建立起正常通信。

步骤五. 配置基于队列的拥塞管理与拥塞避免

为了解决公司总部与分部之间产生的网络拥塞，现在通过配置基于队列的拥塞管理和拥塞避免的方式解决。

在R1上创建WRED丢弃模板**data**，使其基于DSCP优先级进行丢弃，将阀值上限设为90，下限设为50，丢弃概率设为30。

```
[R1]drop-profile data
[R1-drop-profile-data]wred dscp
[R1-drop-profile-data]dscp af32 low-limit 50 high-limit 90 discard-percentage
30
```

在R1上创建队列模板queue-profile1，将数据流量放入WFQ队列，并和丢弃模板data绑定，将需要高优先级，低延迟保证的语音流量放入PQ队列。

```
[R1]qos queue-profile queue-profile1
[R1-qos-queue-profile-queue-profile1]queue 3 drop-profile data
[R1-qos-queue-profile-queue-profile1]schedule wfq 3 pq 5
```

在R1的S1/0/0上应用队列模板。

```
[R1]interface Serial 1/0/0
[R1- Serial0/0/1]qos queue-profile queue-profile1
```

查看配置的队列模板信息。

```
[R1]display qos queue-profile queue-profile1
Queue-profile: queue-profile1
Queue  Schedule  Weight  Length(Bytes/Packets) Gts(CIR/CBS)
-----------------------------------------------------------------
3      WFQ       10              0/0              -/-
5      PQ        -               0/0              -/-
```

此时数据流量与语音流量分别使用了WFQ与PQ队列。

查看配置的丢弃模板信息。

```
[R1]display drop-profile data
Drop-profile[1]: data
DSCP          Low-limit  High-limit  Discard-percentage
-----------------------------------------------------------------
default         30         100         10
1               30         100         10
2               30         100         10
3               30         100         10
```

```
4                 30          100         10
5                 30          100         10
6                 30          100         10
7                 30          100         10
cs1               30          100         10
9                 30          100         10
af11              30          100         10
11                30          100         10
af12              30          100         10
13                30          100         10
af13              30          100         10
15                30          100         10
cs2               30          100         10
17                30          100         10
af21              30          100         10
19                30          100         10
af22              30          100         10
21                30          100         10
af23              30          100         10
23                30          100         10
cs3               30          100         10
25                30          100         10
af31              30          100         10
27                30          100         10
af32              50          90          30
29                30          100         10
af33              30          100         10
31                30          100         10
cs4               30          100         10
33                30          100         10
af41              30          100         10
```

可以观察到配置上限，下限阀值与丢弃概率产生的效果，其余作没有配置的对应的都是默认值。

步骤六. 配置基于流的拥塞管理与拥塞避免

为了解决公司总部与分部之间产生的网络拥塞，现在通过配置基于流的拥塞管理和拥塞避免的方式解决。

现在将公司总部的客户端R4与分部的客户端R3之间的流量定义为重要流量，通过对其做QoS保证，使得R4与R3能够建立正常的通信。

删除步骤五中R1接口S1/0/0上队列模板的调用。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]undo qos queue-profile
```

在R4上使用**ping**命令测试去往R3的连通性，设置源地址为10.0.145.4，包大小为700字节，发10个包。

```
[R4]ping -a 10.0.145.4 -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=1279 ms
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=1587 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=1827 ms
    Request time out
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=1717 ms
    Request time out
    Request time out
    Request time out
    Request time out

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    4 packet(s) received
    60.00% packet loss
    round-trip min/avg/max = 1279/1602/1827 ms
```

此时公司总部与分部之间的链路发生严重拥塞，丢包现象严重，R4无法与R3建立正常通信。

在R1上创建ACL3001匹配从10.0.145.4去往10.0.34.3的流量。

```
[R1]acl number 3001
[R1-acl-adv-3001]rule 0 per ip source 10.0.145.4 0.0.0.0 destination 10.0.34.3 
0.0.0.0
```

创建流分类**class-ef**，匹配ACL3001，创建流行为**behavior-ef**，配置队列调度方式为EF，带宽为10Kbps。

```
[R1]traffic classifier class-ef
[R1-classifier-class-ef]if-match acl 3001
[R1-classifier-class-ef]traffic behavior behavior-ef
[R1-behavior-behavior-ef]queue ef bandwidth 8
```

创建流分类**class-af32**，匹配DSCP值为AF32的数据流量，创建流行为

behavior-af32，配置队列调度方式为AF，带宽为30Kbps，与丢弃模板data绑定。

```
[R1]traffic classifier class-af32
[R1-classifier-class-af32]if-match dscp af32
[R-classifier-class-af321]traffic behavior behavior-af32
[R1-behavior-behavior-af32]queue af bandwidth 30
[R1-behavior-behavior-af32]drop-profile data
```

创建流策略**policy-1**，关联流分类**class-ef**和流动作**behavior-ef**，流分类**class-af32**和流动作**behavior-af32**，并在R1的接口S1/0/0上应用。

```
[R1]traffic policy policy-1
[R1-trafficpolicy-policy-1]classifier class-ef behavior behavior-ef
[R1-trafficpolicy-policy-1]classifier class-af32 behavior behavior-af32
[R1-trafficpolicy-policy-1]interface Serial 1/0/0
[R1-Serial1/0/0]traffic-policy policy-1 outbound
```

在R4上使用**ping**命令测试去往R3的连通性，设置每个包大小为700，源地址为10.0.145.4，个数为10。

```
[R4]ping -a 10.0.145.4 -s 700 -c 10 10.0.34.3
  PING 10.0.34.3: 700  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=700 Sequence=1 ttl=253 time=694 ms
    Reply from 10.0.34.3: bytes=700 Sequence=2 ttl=253 time=391 ms
    Reply from 10.0.34.3: bytes=700 Sequence=3 ttl=253 time=361 ms
    Reply from 10.0.34.3: bytes=700 Sequence=4 ttl=253 time=671 ms
    Reply from 10.0.34.3: bytes=700 Sequence=5 ttl=253 time=211 ms
    Reply from 10.0.34.3: bytes=700 Sequence=6 ttl=253 time=611 ms
    Reply from 10.0.34.3: bytes=700 Sequence=7 ttl=253 time=688 ms
    Reply from 10.0.34.3: bytes=700 Sequence=8 ttl=253 time=391 ms
    Reply from 10.0.34.3: bytes=700 Sequence=9 ttl=253 time=301 ms
    Reply from 10.0.34.3: bytes=700 Sequence=10 ttl=253 time=651 ms

  --- 10.0.34.3 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 211/497/694 ms
```

将R1去往R3的流量设置为EF队列后，现在R1可以与R3建立正常通信。

附加实验：思考并验证

QoS是使用差分服务来实现对不同业务的服务质量的保证，保证带宽和延迟。试想一下，带宽的增加是否可用彻底解决服务质量问题，从而不需要使用QoS？

实验完成后，回想理论课程中关于QoS的逻辑处理过程。将路由器实现QoS的过程总结一下。

最终设备配置

```
<R1>display current-configuration
[V200R001C00SPC200]
#
 sysname R1
#
acl number 3001
 rule 0 permit ip source 10.0.145.4 0 destination 10.0.34.3 0
#
drop-profile data
wred dscp
  dscp af32 low-limit 50 high-limit 90 discard-percentage 30
#
qos queue-profile queue-profile1
  queue 3 drop-profile data
  schedule wfq 3 pq 5
#
qos map-table dscp-dscp
  input 26 output 0
#
traffic classifier class-ef operator or
 if-match acl 3001
traffic classifier class-af32 operator or
 if-match dscp af32
#
traffic behavior behavior-ef
 queue ef bandwidth 10 cbs 250
traffic behavior behavior-af32
 queue af bandwidth 30
 drop-profile data
```

```
traffic behavior behavir-af32
 queue af bandwidth 30
#
traffic policy policy-1
 classifier class-ef behavior behavior-ef
 classifier class-af32 behavior behavior-af32
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 trust dscp
 traffic-policy policy-1 outbound
 baudrate 72000
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.1 255.255.255.0
 trust dscp override
#
 ip route-static 10.0.34.0 255.255.255.0 10.0.12.2
#
Return

<R2>display current-configuration
[V200R001C00SPC200]
#
 sysname R2
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.2 255.255.255.0
#
 ip route-static 10.0.145.0 255.255.255.0 10.0.12.1
#
return

<R3>display current-configuration
[V200R001C00SPC200]
#
 sysname R3
#
```

```
interface GigabitEthernet0/0/2
 ip address 10.0.34.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return

<R4>display current-configuration
[V200R001C00SPC200]
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<R5>display current-configuration
[V200R001C00SPC200]
#
 sysname R5
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.5 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<S3>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S3
#
interface Vlanif1
 ip address 10.0.145.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
nqa test-instance admin udp
 test-type udp
```

```
 destination-address ipv4 10.0.34.4
 destination-port 6000
 tos 28
 frequency 3
 interval seconds 1
 timeout 1
 datasize 5800
 start now
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.0.34.4
 destination-port 6000
 tos 46
 frequency 3
 interval milliseconds 20
 timeout 1
 datasize 90
 start now
#
return

<S4>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S4
#
interface Vlanif1
 ip address 10.0.34.4 255.255.255.0
#
 nqa-server udpecho 10.0.34.4 6000
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return
```

实验 2-2 使用流策略实现流行为控制

学习目的

- 掌握配置端到端QoS的方法
- 掌握使用流策略实现流行为控制的方法

拓扑图

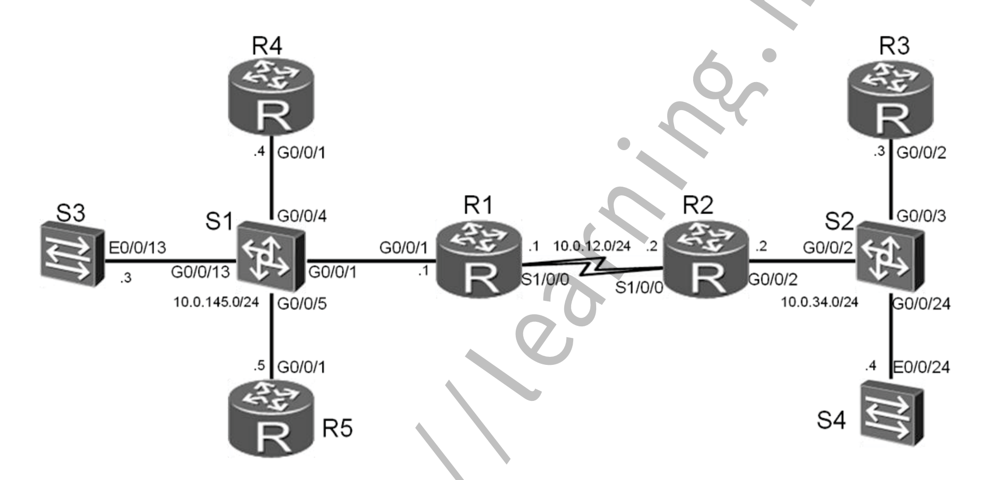


图2-2 使用流策略实现流行为控制

场景

你是公司的网络管理员。公司网络分成两部分，其中R1与S1在公司总部，R2与S2在公司分部，之间通过专线实现互联。随着网络的发展，内网带宽逐渐增大，而专线的带宽一直没有升级，所以网络中出现了比较严重的重要业务反应较慢，或无法正常使用的情况。

部署端到端QoS，你可以调整相应的QoS特性，保证重要的业务数据能更好的发送到目标，并通过流策略实现对流行为的控制。

学习任务

步骤一. 基础配置与 IP 编址

给所有路由器和交换机S3，S4配置IP地址和掩码。

```
<R1>system-view
Enter system view, return user view with Ctrl+Z.
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]ip address 10.0.12.1 255.255.255.0
[R1-Serial1/0/0]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]ip add 10.0.145.1 255.255.255.0

<R2>system-view
Enter system view, return user view with Ctrl+Z.
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]ip address 10.0.12.2 255.255.255.0
[R2-Serial1/0/0]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]ip address 10.0.34.2 255.255.255.0

<R3>system-view
Enter system view, return user view with Ctrl+Z.
[R3]interface GigabitEthernet 0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.0.34.3 255.255.255.0

<R4> system-view
Enter system view, return user view with Ctrl+Z.
[R4]interface GigabitEthernet 0/0/1
[R4-GigabitEthernet0/0/1]ip address 10.0.145.4 255.255.255.0

<R5>system-view
Enter system view, return user view with Ctrl+Z.
[R5]interface GigabitEthernet 0/0/1
[R5-GigabitEthernet0/0/1]ip address 10.0.145.5 255.255.255.0

<S3>system-view
Enter system view, return user view with Ctrl+Z.
[S3]interface Vlanif 1
[S3-Vlanif1]ip address 10.0.145.3 255.255.255.0

<S4>system-view
Enter system view, return user view with Ctrl+Z.
```

```
[S4]interface Vlanif 1
[S4-Vlanif1]ip address 10.0.34.4 255.255.255.0
```

配置完成后，测试直连链路的连通性。

```
[R1]ping -c 1 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.12.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms

[R1]ping -c 1 10.0.145.3
  PING 10.0.145.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.3: bytes=56 Sequence=1 ttl=255 time=35 ms

  --- 10.0.145.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/35/35 ms

[R1]ping -c 1 10.0.145.4
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms

[R1]ping -c 1 10.0.145.5
  PING 10.0.145.5: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.5: bytes=56 Sequence=1 ttl=255 time=6 ms

  --- 10.0.145.5 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/6/6 ms
```

```
[R2]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=255 time=5 ms

  --- 10.0.34.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 5/5/5 ms

[R2]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=255 time=36 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 36/36/36 ms
```

步骤二. 配置静态路由

在所有路由器和交换机S3，S4上配置静态路由。

```
[R1]ip route-static 10.0.34.0 255.255.255.0 10.0.12.2

[R2]ip route-static 10.0.145.0 255.255.255.0 10.0.12.1

[R3]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2

[R4]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[R5]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S3]ip route-static 0.0.0.0 0.0.0.0 10.0.145.1

[S4]ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
```

配置完成后，测试网络连通性。

```
[S3]ping -c 1 10.0.34.4
  PING 10.0.34.4: 56  data bytes, press CTRL_C to break
```

```
    Reply from 10.0.34.4: bytes=56 Sequence=1 ttl=252 time=40 ms

  --- 10.0.34.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/40/40 ms

[R4]ping -c 1 10.0.34.3
  PING 10.0.145.4: 56  data bytes, press CTRL_C to break
    Reply from 10.0.145.4: bytes=56 Sequence=1 ttl=255 time=3 ms

  --- 10.0.145.4 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

[R5]ping -c 1 10.0.34.3
  PING 10.0.34.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.34.3: bytes=56 Sequence=1 ttl=253 time=44 ms

  --- 10.0.34.3 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 44/44/44 ms
```

步骤三.　配置 DSCP 优先级的重标记

公司网络中有语音，视频，数据三种业务，但是由于公司总部与分部之间的专线仍然没有得到升级，所以不可避免网络出现了拥塞。

通过配置端到端的QoS来实现语音报文的优先发送，视频报文的带宽保证。

将R4与R3之间的流量模拟为语音报文，将R5与R3之间的流量模拟为视频报文，将S3与S4之间的报文模拟为数据报文。接下来将针对语音报文和视频报文做一系列相关的QoS策略，对数据报文默认尽最大努力传输。

现在将语音报文的DSCP值标记为EF，视频报文的DSCP值标记为AF32。

在S1上创建ACL3001，3002，分别匹配R4去往R3，R5去往R3的流量。

```
[S1]acl number 3001
```

```
[S1-acl-adv-3001]rule 0 permit ip source 10.0.145.4 0 destination 10.0.34.3 0
[S1-acl-adv-3001]acl number 3002
[S1-acl-adv-3002]rule 0 permit ip source 10.0.145.5 0 destination 10.0.34.3 0
```

在S1上创建流分类class-voice-s1，匹配ACL3001。创建流行为behavior-voice-s1，将DSCP优先级重标记为EF。

创建流策略policy-voice-s1，关联流分类class-voice-s1与流行为behavior-voice-s1，在接口G0/0/4的入方向上调用该流策略。

```
[S1]traffic classifier class-voice-s1
[S1-classifier-class-voice-s1]if-match acl 3001
[S1-classifier-class-voice-s1]traffic behavior behavior-voice-s1
[S1-behavior-behavior-voice-s1]remark dscp ef
[S1-behavior-behavior-voice-s1]traffic policy policy-voice-s1
[S1-trafficpolicy-policy-voice-s1]classifier class-voice-s1 behavior
behavior-voice-s1
[S1-trafficpolicy-policy-voice-s1]interface GigabitEthernet 0/0/4
[S1-GigabitEthernet0/0/4]traffic-policy policy-voice-s1 inbound
```

在S1上创建流分类class-video-s1，匹配ACL3002。创建流行为behavior-video-s1，将DSCP优先级重标记为AF32。创建流策略policy-video-s1，关联流分类class-video-s1与流行为behavior-video-s1，在接口G0/0/5的入方向上应用该流策略。

```
[S1]traffic classifier class-video-s1
[S1-classifier-class-video-s1]if-match acl 3002
[S1-classifier-class-video-s1]traffic behavior behavior-video-s1
[S1-behavior-behavior-video-s1]remark dscp af32
[S1-behavior-behavior-video-s1]traffic policy policy-video-s1
[S1-trafficpolicy-policy-video-s1]classifier class-video-s1 behavior
behavior-video-s1
[S1-trafficpolicy-policy-video-s1]interface GigabitEthernet 0/0/5
[S1-GigabitEthernet0/0/5]traffic-policy policy-video-s1 inbound
```

在S2上创建ACL3001，3002，分别匹配R3去往R4，R3去往R5的流量。

```
[S2]acl number 3001
[S2-acl-adv-3001]rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.4 0
[S2-acl-adv-3001]acl number 3002
[S2-acl-adv-3002]rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.5 0
```

在S2上创建流分类class-voice-s2，匹配ACL3001。创建流行为behavior-voice-s2，将DSCP优先级重标记为EF。

```
[S2]traffic classifier class-voice-s2
```

```
[S2-classifier-class-voice-s2]if-match acl 3001
[S2-classifier-class-voice-s2]traffic behavior behavior-voice-s2
[S2-behavior-behavior-voice-s2]remark dscp ef
```

在S2上创建流分类class-video-s2，匹配ACL3002。创建流行为behavior-video-s2，将DSCP优先级重标记为AF32。

```
[S2]traffic classifier class-video-s2
[S2-classifier-class-video-s2]if-match acl 3002
[S2-classifier-class-video-s2]traffic behavior behavior-video-s2
[S2-behavior-behavior-video-s2]remark dscp af32
```

在S2上创建流策略policy-voice-video-s2，关联流分类class-voice-s2与流行为behavior-voice-s2，关联流分类class-video-s2与流行为behavior-video-s2，在接口G0/0/3的入方向上应用该流策略。

```
[S2]traffic policy policy-voice-video-s2
[S2-trafficpolicy-policy-voice-video-s2]classifier class-voice-s2 behavior
behavior-voice-s2
[S2-trafficpolicy-policy-voice-video-s2]classifier class-video-s2 behavior
behavior-video-s2
[S2]interface GigabitEthernet 0/0/3
[S2-GigabitEthernet0/0/3]traffic-policy policy-voice-video-s2 inbound
```

步骤四. 配置流量整形和监管

在公司总部和分部的核心交换机上部署流量整形，缓解流量拥塞。

在S1的接口G0/0/1出方向上配置流量整形，CIR设为128kbit/s。

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]qos lr outbound cir 128
```

查看流量整形配置信息。

```
[S1]display qos lr outbound interface GigabitEthernet 0/0/1
GigabitEthernet0/0/1 lr outbound:
  cir: 128 Kbps, cbs: 16000 Byte
```

在S2的接口G0/0/2出方向上配置流量整形，CIR设为128kbit/s。

```
[S2]interface GigabitEthernet 0/0/2
[S2-GigabitEthernet0/0/2]qos lr outbound cir 128
```

查看流量整形配置信息。

```
[S2]display qos lr outbound interface GigabitEthernet 0/0/2
GigabitEthernet0/0/2 lr outbound:
  cir: 128 Kbps, cbs: 16000 Byte
```

在公司总部和分部的出口路由器上部署流量监管，进一步缓解流量拥塞。

在R1的接口G0/0/1入方向上配置流量监管，CIR设为72kbit/s。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]qos car inbound cir 72
```

在R2的接口G0/0/2入方向上配置流量监管，CIR设为72kbit/s。

```
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]qos car inbound cir 72
```

步骤五. 配置基于流策略的拥塞管理与拥塞避免

在公司总部与分部的出口路由器上部署基于流策略的拥塞管理与拥塞避免。保证语音流量低延迟，优先发送，保证视频流量拥有足够的带宽。

配置R1的接口G0/0/1信任DSCP优先级。

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]trust dscp
```

在R1上创建WRED丢弃模板video-r1，使其基于DSCP优先级进行丢弃，将阀值下限设为50，上限设为90，丢弃概率设为30，

```
[R1]drop-profile video
[R1-drop-profile-video-r1]wred dscp
[R1-drop-profile-video-r1]dscp af32 low-limit 50 high-limit 90
discard-percentage 30
```

在R1上创建流分类class-af32-r1，匹配DSCP值为AF32的视频流量。创建流行为behavior-af32-r1，配置队列调度方式为AF，最大带宽占接口带宽百分比设为40，并与丢弃模板video-r1绑定。

```
[R1]traffic classifier class-af32-r1
[R1-classifier-class-af32-r1]if-match dscp af32
[R1-classifier-class-af32-r1]traffic behavior behavior-af32-r1
[R1-behavior-behavior-af32-r1]queue af bandwidth pct 40
[R1-behavior-behavior-af32-r1]drop-profile video-r1
```

在R1上创建流分类class-ef-r1，匹配DSCP值为EF的语音流量。创建流行为behavior-ef-r1，配置队列的调度方式为EF，最大带宽占接口带宽百分比设为30。

```
[R1]traffic classifier class-ef-r1
[R1-classifier-class-ef-r1]if-match dscp ef
[R1-classifier-class-ef-r1]traffic behavior behavior-ef-r1
[R1-behavior-behavior-ef-r1]queue ef bandwidth pct 30
```

在R1上创建流策略policy-r1，关联流分类class-af32-r1与流行为behavior-af32-r1，关联流分类class-ef-r1与流行为behavior-ef-r1，并在接口S1/0/0的出方向上应用。

```
[R1]traffic policy policy-r1
[R1-trafficpolicy-policy-r1]classifier class-af32-r1 behavior behavior-af32-r1
[R1-trafficpolicy-policy-r1]classifier class-ef-r1 behavior behavior-ef-r1
[R1-trafficpolicy-policy-r1]interface Serial 1/0/0
[R1-Serial1/0/0]traffic-policy policy-r1 outbound
```

在公司总部R1上配置完后，在公司分部R2上也作相应配置。

配置R2的接口G0/0/2信任DSCP优先级。

```
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]trust dscp
```

在R2上创建WRED丢弃模板video-r2，使其基于DSCP优先级进行丢弃，将阀值下限设为50，上限设为90，丢弃概率设为30，

```
[R2]drop-profile video-r2
[R2-drop-profile-video-r2]wred dscp
[R2-drop-profile-video-r2]dscp af32 low-limit 50 high-limit 90
discard-percentage 30
```

在R1上创建流分类class-af32-r2，匹配DSCP值为AF32的视频流量。创建流行为behavior-af32-r2，配置队列调度方式为AF，最大带宽占接口带宽百分比设为40，并与丢弃模板video-r2绑定。

```
[R2]traffic classifier class-af32-r2
[R2-classifier-class-af32-r2]if-match dscp af32
[R2-classifier-class-af32-r2]traffic behavior behavior-af32-r2
[R2-behavior-behavior-af32-r2]queue af bandwidth pct 40
[R2-behavior-behavior-af32-r2]drop-profile video-r2
```

在R1上创建流分类class-ef-r2，匹配DSCP值为EF的语音流量。创建流行为behavior-ef-r2，配置队列的调度方式为EF，最大带宽占接口带宽百分比设为30。

```
[R2]traffic classifier class-ef-r2
[R2-classifier-class-ef-r2]if-match dscp ef
[R2-classifier-class-ef-r2]traffic behavior behavior-ef-r2
[R2-behavior-behavior-ef-r2]queue ef bandwidth pct 30
```

在R1上创建流策略policy-r2，关联流分类class-af32-r2与流行为behavior-af32-r2，关联流分类class-ef-r1与流行为behavior-ef-r2，并在接口S1/0/0的出方向上应用。

```
[R2]traffic policy policy-r2
[R2-trafficpolicy-policy-r2]classifier class-af32-r2 behavior behavior-af32-r2
[R2-trafficpolicy-policy-r2]classifier class-ef-r2 behavior behavior-ef-r2
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]traffic-policy policy-r2 outbound
```

步骤六. 配置基于流策略实现流行为控制

公司总部现在出于优化的的目的将针对部分流量做控制，丢弃掉UDP端口号4000至5000部分的视频流量。

在R1上创建ACL3003，匹配从R5去往R3，UDP端口范围为4000至5000部分的流量。

```
[R1]acl number 3003
[R1-acl-adv-3003]rule 0 permit udp source-port range 4000 5000 source 10.0.145.5
0 destination 10.0.34.3 0
```

在R1上创建流分类class-drop，匹配ACL3003，

```
[R1]traffic classifier class-drop
[R1-classifier-class-drop]if-match acl 3003
```

在R1上创建流行为behavior-drop，配置命令**deny**，执行禁止动作，

```
[R1]traffic behavior behavior-drop
[R1-behavior-behavior-drop]deny
```

在R1上创建流策略policy-drop，关联流分类class-drop与流行为behavior-drop，并在接口G0/0/5的入方向上应用。

```
[R1]traffic policy policy-drop
[R1-trafficpolicy-policy-drop]classifier class-drop behavior behavior-drop
[R1-trafficpolicy-policy-drop]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]traffic-policy policy-drop inbound
```

查看配置信息。

```
[R1]dis traffic policy user-defined policy-drop
  User Defined Traffic Policy Information:
    Policy: policy-drop
    Classifier: class-drop
    Operator: OR
     Behavior: behavior-drop
     Deny
```

附加实验：思考并验证

实验完成后，回顾QoS的知识框架，总结QoS中各项策略的使用范围与应用场景。

最终设备配置

```
<R1>display current-configuration
[V200R001C00SPC200]
#
 sysname R1
#
acl number 3003
 rule 0 permit udp source 10.0.145.5 0 source-port range 4000 5000 destination
10.0.34.3 0
#
drop-profile video-r1
wred dscp
  dscp af32 low-limit 50 high-limit 90 discard-percentage 30
#
traffic classifier class-drop operator or
 if-match acl 3003
traffic classifier class-ef-r1 operator or
 if-match dscp ef
traffic classifier class-af32-r1 operator or
 if-match dscp af32
#
traffic behavior behavior-af32-r1
 queue af bandwidth pct 40
 drop-profile video-r1
traffic behavior behavior-ef-r1
```

```
 queue ef bandwidth pct 30
traffic behavior behavior-drop
 deny
#
traffic policy policy-drop
 classifier class-drop behavior behavior-drop
traffic policy policy-r1
 classifier class-af32-r1 behavior behavior-af32-r1
 classifier class-ef-r1 behavior behavior-ef-r1
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.1 255.255.255.0
 traffic-policy policy-r1 outbound
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.1 255.255.255.0
 trust dscp
 qos car inbound cir 72 cbs 13536 pbs 22536 green pass yellow pass red discard
 traffic-policy policy-drop inbound
#
 ip route-static 10.0.34.0 255.255.255.0 10.0.12.2
#
return

<R2>display current-configuration
[V200R001C00SPC200]
#
 sysname R2
#
drop-profile video-r2
wred dscp
  dscp af32 low-limit 50 high-limit 90 discard-percentage 30
#
traffic classifier class-ef-r2 operator or
 if-match dscp ef
traffic classifier class-af32-r2 operator or
 if-match dscp af32
#
traffic behavior behavior-af32-r2
 queue af bandwidth pct 40
 drop-profile video-r2
traffic behavior behavior-ef-r2
```

```
 queue ef bandwidth pct 30
#
traffic policy policy-r2
 classifier class-af32-r2 behavior behavior-af32-r2
 classifier class-ef-r2 behavior behavior-ef-r2
#
interface Serial1/0/0
 link-protocol ppp
 ip address 10.0.12.2 255.255.255.0
 traffic-policy policy-r2 outbound
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.2 255.255.255.0
 trust dscp
 qos car inbound cir 72 cbs 13536 pbs 22536 green pass yellow pass red discard
#
 ip route-static 10.0.145.0 255.255.255.0 10.0.12.1
#
return

<R3>display current-configuration
[V200R001C00SPC200]
#
 sysname R3
#
interface GigabitEthernet0/0/2
 ip address 10.0.34.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return

<R4>display current-configuration
[V200R001C00SPC200]
#
 sysname R4
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return
```

```
<R5>display current-configuration
[V200R001C00SPC200]
#
 sysname R5
#
interface GigabitEthernet0/0/1
 ip address 10.0.145.5 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<S1>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S1
#
acl number 3001
 rule 0 permit ip source 10.0.145.4 0 destination 10.0.34.3 0
acl number 3002
 rule 0 permit ip source 10.0.145.5 0 destination 10.0.34.3 0
#
traffic classifier class-video-s1 operator and
 if-match acl 3002
traffic classifier class-voice-s1 operator and
 if-match acl 3001
#
traffic behavior behavior-video-s1
 remark dscp af32
traffic behavior behavior-voice-s1
 remark dscp ef
#
traffic policy policy-video-s1
 classifier class-video-s1 behavior behavior-video-s1
traffic policy policy-voice-s1
 classifier class-voice-s1 behavior behavior-voice-s1
#
interface GigabitEthernet0/0/1
 qos lr outbound cir 128 cbs 16000
#
interface GigabitEthernet0/0/4
 traffic-policy policy-voice-s1 inbound
```

```
#
interface GigabitEthernet0/0/5
 traffic-policy policy-video-s1 inbound
#
return

<S2>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S2
#
acl number 3001
 rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.4 0
acl number 3002
 rule 0 permit ip source 10.0.34.3 0 destination 10.0.145.5 0
#
traffic classifier class-video-s2 operator and
 if-match acl 3002
traffic classifier class-voice-s2 operator and
 if-match acl 3001
#
traffic behavior behavior-video-s2
 remark dscp af32
traffic behavior behavior-voice-s2
 remark dscp ef
#
traffic policy policy-voice-video-s2
 classifier class-voice-s2 behavior behavior-voice-s2
 classifier class-video-s2 behavior behavior-video-s2
#
interface GigabitEthernet0/0/2
 qos lr outbound cir 128 cbs 16000
#
interface GigabitEthernet0/0/3
 traffic-policy policy-voice-video-s2 inbound
#
return

<S3>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S3
#
```

```
interface Vlanif1
 ip address 10.0.145.3 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.145.1
#
return

<S4>display current-configuration
#
!Software Version V100R006C00SPC800
 sysname S4
#
interface Vlanif1
 ip address 10.0.34.4 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.0.34.2
#
return
```

第三章 综合实验

实验 3-1 综合实验 1（选做）

学习目的

- 掌握MST的配置方法
- 掌握VLAN间路由的配置方法
- 掌握RIP的配置方法
- 掌握OSPF的配置方法
- 掌握路由引入的配置方法
- 掌握路由策略的配置方法
- 掌握防火墙的配置方法
- 掌握交换机上QOS的配置方法

拓扑图

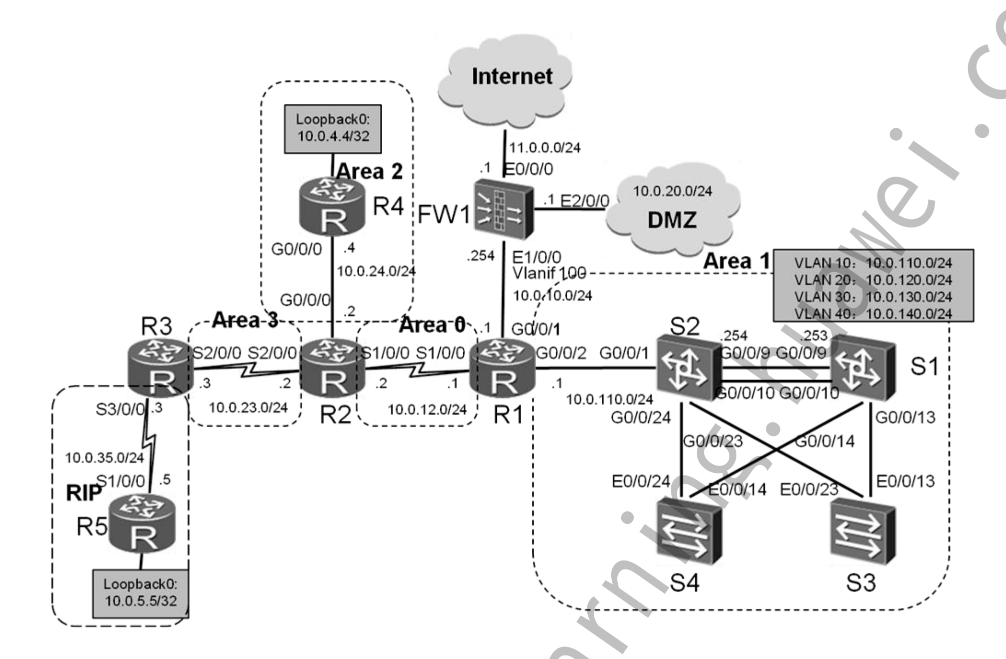


图 3-1 综合实验1（选做）

场景

你是公司的网络管理员。公司的网络由一个总部网络区域，一个分部网络区域和一个分支办公室网络区域组成。

其中总部网络区域由一台防火墙、一台路由器和四台交换机组成。防火墙控制公司内部网络与外部网络之间的互访，将网络划分为Trust、Untrust和DMZ三个区域。四台交换机使用MST技术实现网络冗余，提高网络可靠性。并使用QOS技术在交换网络上对数据流进行优化。

总部网络和分支办公室网络的路由器使用专线相连，同处于OSPF路由域中。为了优化OSPF路由域，将总部网络和分支办公室网络配置为OSPF末节区域型网络。由于分支机构使用的网络协议为RIP，需要在OSPF边界使用路由引入，以实现RIP路由域和OSPF路由域的互通。

学习任务

由于本综合实验的目的在于检测学员对前面实验学习掌握的程度，所以仅给出大概步骤和验证方式，不给出具体的操作命令。

步骤一. 基础配置与 IP 编址

给所有设备配置IP地址和掩码，配置完成后测试直连设备的连通性。

步骤二. MST 配置

交换机S1与S2之间连线为Eth-trunk链路。

将交换机与交换机之间连线的接口模式改为Trunk模式，并允许VLAN 10/20/30和40通过。

在所有交换机上都创建VLAN 10、20、30、40、100，同时配置MST生成两个实例。VLAN 10、VLAN 20和VLAN 100以S1为根，VLAN 30和VLAN 40以S2为根。

步骤三. VLAN 间路由配置

将S1的G0/0/22和G0/0/1接口加入VLAN 100，将S2的G0/0/1接口加入VLAN 10。

在S1和S2上为VLAN 10、20、30、40创建相应Vlanif接口，实现VLAN间通信。

步骤四. OSPF 配置

在R1、R2、R3、R4和S1、S2上配置OSPF路由协议。将R1和R2之间的链路配置属于OSPF区域0。总部网络配置属于OSPF区域1，分支办公室网络配置属于OSPF区域2，同时将区域1和区域2配置为OSPF末节区域。将R2与R3相连网络配置属于区域3 ,并将区域3配置为NSSA区。R1连接FW1的网络不运行OSPF。

步骤五. 路由引入配置

在R3和R5上配置RIP路由协议。在R3上使用路由引入，配置RIP路由域和OSPF路由域互相引入，实现RIP路由域和OSPF路由域之间的互通。在将RIP路由引入OSPF路由域的时候使用路由策略控制只引入R5连接的网络，而不把R3与R2直接的网络引入OSPF路由域。

在FW1上创建VLAN 100及相应的Vlanif接口，并按照拓扑图所示配置IP地址。在R1上配置一条缺省路由，下一跳地址为FW1的Vlanif 100接口地址。同时将这条路由信息引入OSPF，并让R5学习到。

同时在FW1上创建静态路由10.0.0.0/16，下一跳地址为R1的G0/0/1接口地址。使FW1能够和企业内网所有设备通信。

步骤六. 防火墙配置

按拓扑图所示，将FW1上相应端口分别加入Trust、Untrust和DMZ区域中。实现Trust区域可以访问所有区域的内容，Untrust区域只能访问DMZ区域中的服务器10.0.20.1的80号端口。DMZ区域不能主动访问所有区域。

步骤七. 网络优化配置

连接在交换机S4上的用户有些需要限制数据传输速度，有些需要提高数据传输优先级。E0/0/1接口属于VLAN 10，E0/0/2属于VLAN 30。请将S4的E0/0/1接口传输速度限制为128Kb。将E0/0/2接口的报文DSCP值修改为45，并设置E0/0/2信任报文的DSCP值。

附加实验：思考并验证

综合实验更贴近实际场景，对比之前的实验与这个实验，简述有哪些差异。

最终设备配置

```
[R1]display current-configuration
```

```
[R2]display current-configuration
```

```
[R3]display current-configuration
```

```
[R4]display current-configuration
```

```
[R5]display current-configuration
```

```
[S1]display current-configuration
```

```
[S2]display current-configuration
```

```
[S3]display current-configuration
```

```
[S4]display current-configuration
```

```
[FW1]display current-configuration
```

实验 3-2 综合实验 2（选做）

实验目标

- 掌握IBGP，EBGP的配置方法
- 掌握BGP属性的配置方法
- 掌握SEP的配置方法
- 掌握USG防火墙上NAT，IPSec的配置方法
- 掌握路由器上端到端QoS的配置方法

拓扑图

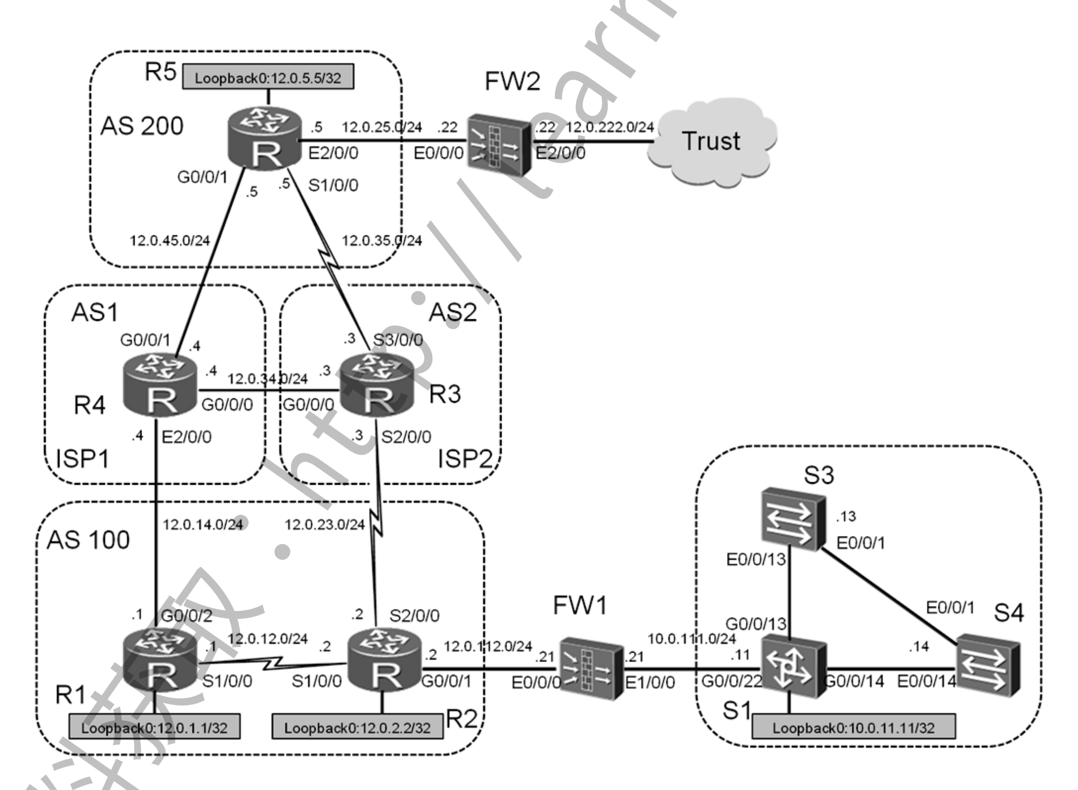


图3-2 综合实验2（选做）

场景

你是公司的管理员。公司总部与分部之间使用BGP协议通过两个不同的运营商ISP1，ISP2相连，其中公司总部使用AS号100，分部使用AS号200，ISP1的AS号为1，ISP2的AS号为2。

公司使用ISP1作为主用链路，ISP2作为备用链路。公司总部的核心交换网与出口路由器之间部署了USG防火墙，交换网络中使用SEP协议提供冗余保护，公司总部与分部的防火墙之间建立IPSec VPN。

学习任务

步骤一. 基础配置与 IP 编址

给所有路由器配置物理接口及Loopback接口的IP地址和掩码，配置完成后，测试直连链路的连通性。注意各Loopback 0接口均使用32位掩码。

步骤二. 配置 BGP

在R1，R2，R3，R4，R5上配置IBGP与EBGP，全部使用物理接口地址建立对等体关系，AS规划如图所示。由于默认情况下，BGP的负载分担是关闭的，为了避免影响选路，在所有的路由器上打开负载分担，设置为最大4条路径。

在R1，R2，R5上将各自的环回接口地址所在的网段发布进BGP中，查看BGP路由表，此时R5都是通过R3学习到12.0.1.1/32与12.0.2.2/32，R1从R4学习到12.0.5.5/32，R2从R3学习到12.0.5.5/32。

现在希望公司总部与分部之间的通信全部使用ISP1的主用链路。

在R5上创建路由策略**as_path**，针对从对等体R3学习到的12.0.1.1/32与12.0.2.2/32这两条路由的AS-PATH属性，增加2个重复的AS号100。查看BGP路由表，此时R5从R4学习到这两条路由。

在R1上创建路由策略**local_pref**，将路由12.0.5.5/32的本地优先级属性修改为200，然后将策略应用到IBGP对等体R2上。观察R2上的路由表，此时R2选择从R4学习路由12.0.5.5/32。

步骤三. 配置 SEP

为了提升网络的健壮性，交换机S1、S2和S3采用了冗余连接。在连接中形成了一个闭合环路。使用SEP协议为这个网络环路提供冗余保护。

关闭S1，S2的G0/0/9，G0/0/10接口，S3的E0/0/23接口，S4的E0/0/14接口，避免对实验造成影响。

创建SEP段，并配置控制VLAN100和指定保护实例为**all**。

将S1的G0/0/13，G0/0/14接口加入SEP段，将G0/0/13设为主边缘接口，G0/0/14设为副边缘接口，将S3和S4的接口都加入SEP段。

在主边缘接口位于的设备S1上配置阻塞端口的方式为依据端口优先级。

配置S3上的接口E0/0/1的优先级为128。

在主边缘端口位于的设备S1上配置抢占模式为延时抢占，延时为30s。

配置完成后，查看SEP运行信息，S3的E0/0/1接口应该为阻塞状态。

步骤四. 配置防火墙 NAT

在公司总部的核心交换网与出口路由器之间的防火墙FW1上做配置，实现NAT。

在S1上创建VLAN10，将接口G0/0/22加入VLAN10中，配置Vlanif10地址为10.0.111.11/24。在FW1上配置VLAN10，定义Vlanif10，配置IP地址作为Trust区域的网关，使用IP地址10.0.111.21/24。另外由于默认情况下防火墙会给它的Vlanif1配置地址，实验中为避免干扰，删除该配置。

在R2上将路由12.0.112.0/24发布进BGP。在R2上配置默认路由，下一跳指

向FW1，并引入BGP中，在FW1上配置默认路由，下一跳指向R2，在S1上配置默认路由，下一跳指向FW1。

在FW1上将接口E0/0/0配置到Untrust区域，将接口E1/0/0配置到Trust区域，配置区域间的安全过滤，从Trust区域的网段10.0.111.0/24发往Untrust区域的数据包被放行。

在FW1配置使用Easy-IP，针对10.0.111.0/24进行NAT源地址转换。并且将NAT与接口E0/0/0进行绑定。

配置完成后，FW1上的Trust区域的网段与Untrust区域的网段可以正常访问。

步骤五. 配置防火墙 IPSec VPN

在公司总部与分部的防火墙FW1与FW2之间实现IPSec VPN。

配置防火墙FW2的Ethernet 2/0/0的接口地址。在FW2上，将E0/0/0加入到Untrust区域，将E2/0/0加入到Trust区域。在FW1和FW2上配置从Trust区域发往Untrust区域的数据包被放行。从Untrust区域发往Local区域的数据包被放行。

将路由12.0.5.0/24发布进BGP，在FW2上配置默认路由，下一跳指向R5，在FW1上配置去往12.0.222.0/24的静态路由，在FW2上配置去往10.0.111.0/24的静态路由。

在FW1和FW2上定义各自要保护的数据流。在FW1上配置ACL3000，匹配从10.0.111.0/24去往12.0.222.0/24的流量，在FW2上配置ACL3000,匹配从12.0.222.0/24去往10.0.111.0/24的流量。

在防火墙FW1和FW2上配置IPSec安全提议。IPSec协议的封装模式为隧道模式，IPSec的安全协议为ESP，ESP协议的加密算法为DES。在防火墙FW1和FW2上配置IKE安全提议，IKE的认证算法为SHA1，加密算法为DES。

在防火墙FW1和FW2上配置IKE对等体，IKE对等体默认使用IKEv2协商方式。

在防火墙FW1和FW2上配置安全策略。并在防火墙FW1和FW2的接口E0/0/0上应用安全策略。

此时FW1与FW2之间的IPSec VPN建立。

步骤六. 配置 QoS

公司总部R1，R2与分部R5之间的流量全部从ISP1的主用链路走，部署QoS来避免可能出现的拥塞。

在R1上创建ACL3001，3002分别匹配从R1去往R5和R2去往R5的流量，

在R1上创建流分类**class_r1_r2**，匹配ACL3001，3002，创建流行为**behavior_r1_r2** ,配置流量整形动作 ,CIR设为10000 ,创建流策略**policy_r1_r2**，关联流分类**class_r1_r2**和流行为**behavior_r1_r2**，并在接口G0/0/2的出方向上应用。

在R4的接口G0/0/2，G0/0/1上配置基于接口的流量监管，CIR设为8000。

在R5上创建ACL3001，3002分别匹配从R5去往R1和R5去往R2的流量，

在R5上创建流分类**class_r5**，匹配ACL3001，3002，创建流行为**behavior_r5**，配置流量整形动作，CIR设为10000，创建流策略**policy_r5**，关联流分类**class_r5**和流行为**behavior_r5**，并在接口G0/0/1的出方向上应用。

附加实验：思考并验证

最终设备配置

```
[R1]display current-configuration
```

```
[R2]display current-configuration

[R3]display current-configuration

[R4]display current-configuration

[R5]display current-configuration

[S1]display current-configuration

[S2]display current-configuration

[S3]display current-configuration

[S4]display current-configuration

[FW1]display current-configuration
```

在线学习资料支持

您可以在华为企业业务网站获得E-Learning课程、培训教材 、产品资料、软件工具、技术案例等:

1、 E-Learning课程：登录*华为在线学习网站*，进入“*华为培训/在线学习*”栏目

免费E-Learning课：对网站所有用户免费开放

职业认证E-Learning课：通过任何一项职业认证即可学习所有职业认证培训E-Learning课程

渠道赋能E-Learning课：对华为企业业务合作伙伴免费开放

2、培训教材：登录*华为在线学习网站*，进入“*华为培训/面授培训*”， 在具体课程页面即可下载教材。

华为职业认证培训教材、华为产品技术培训教材。无需注册即可下载

3、华为在线公开课(LVC)： http://support.huawei.com/ecommunity/bbs/10154479.html

企业网络、UC&C、安全、存储等诸多领域的职业认证课程，华为讲师公开授课

4、产品资料下载： http://support.huawei.com/enterprise/#tabname=productsupport

5、软件工具下载：http://support.huawei.com/enterprise/#tabname=softwaredownload

更多内容请访问：

- http://learning.huawei.com/cn
- http://support.huawei.com/enterprise/
- http://support.huawei.com/ecommunity/